



BULLETIN (SB22-003)
VULNERABILITY SUMMARY FOR THE WEEK OF
27TH DECEMBER, 2021



Bulletin (SB22-003) Vulnerability Summary for the Week of December 27, 2021

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.

Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -

Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
@fastify/aws-lambda-- @fastify/aws-lambda	@fastify/aws-lambda version 6.4.0 decorates each Fastify request with request.awsLambda.event and request.awsLambda.context, values that applications are documented to use for authorization decisions such as reading API Gateway authorizer claims. In the default configuration, the getter that populates this decoration reads the client-controlled x-apigateway-event and x-apigateway-context HTTP headers before falling back to the trusted internal request token, and those reserved headers are not stripped from the incoming event. An unauthenticated attacker who can set a single HTTP header can therefore forge the entire Lambda proxy event, including the authorizer context, and override the genuine one. This results in a full authentication and authorization bypass and privilege escalation for any application that trusts request.awsLambda.event for identity or access control. Only version 6.4.0 is affected. Patches: upgrade to @fastify/aws-lambda 6.4.1, which resolves the decoration only through the internal per-invocation token and strips the reserved headers before the request is processed.	2026-08-03	9.1	CVE-2026-18248
@fastify/static-- @fastify/static	@fastify/static before version 10.1.3 contains an incomplete fix for a previous route guard bypass. The static file handler rejected only parent directory segments, but it did not canonicalize dot segments, duplicate slashes, encoded dots, or backslashes before route matching and before delegating to the send layer. As a result, an unauthenticated attacker could request a file protected by a route based guard using a non canonical path form that misses the guarded route yet resolves back onto the protected file, disclosing its contents. Applications that protect a subtree of the static root with a route based guard are affected, while applications relying on the allowedPath option are not. This is fixed in @fastify/static 10.1.3, which canonicalizes the pathname, including rejecting backslashes, on the path used for routing and serving.	2026-08-06	7.5	CVE-2026-18427
@msykes--Events Manager	Unauthenticated Cross Site Scripting (XSS) in Events Manager <= 7.4.1 versions.	2026-08-06	7.1	CVE-2026-66457
absmach--magistrala	Magistrala's Rules Engine allows authenticated users to create rules with embedded Go or Lua scripts executed server-side when IoT messages arrive. The Go script engine (re/golang.go) runs scripts through the Yaegi interpreter with stdlib.Symbols, exposing the full Go standard library (including os and net/http) with validation limited to a regex blocking goroutines and panic() calls; dangerous functions such as os.ReadFile, os.WriteFile, os.Remove, and os.Environ remain fully accessible. The Lua script engine (re/lua.go) performs no input validation at all and preloads dangerous libraries: db (arbitrary database access), ioutil (file I/O), an HTTP client (SSRF), and filepath (traversal). An authenticated low-privileged user can achieve arbitrary file read/write, environment variable leakage, database access, and SSRF against internal microservices.	2026-08-05	8.8	CVE-2026-71235
absmach--magistrala	Magistrala (formerly Mainflux)'s message-readers API reads a `format` value from the HTTP query string (readers/api/http/transport.go) with no validation and interpolates it directly into raw SQL queries via fmt.Sprintf() in both the PostgreSQL reader (readers/postgres/messages.go: `fmt.Sprintf("SELECT * FROM %s WHERE %s ...", format, cond)`) and the TimescaleDB reader (readers/timescale/messages.go, same pattern), enabling SQL injection by any authenticated user able to query channel messages.	2026-08-05	7.1	CVE-2026-71276
Acrisure--KARR BT	The KARR Security System and SWDS dealer-installed automotive anti-theft systems use a shared Bluetooth authentication key across affected devices. An attacker within Bluetooth range can leverage this weakness to issue unauthorized commands to the vehicle, potentially allowing unauthorized access to vehicle functions, including door unlocking and engine immobilization.	2026-08-05	8.1	CVE-2026-18411
adafap--api-mcp	A security vulnerability has been detected in adafap api-mcp up to 92b9a5d04acfec165c7d4ef852496593aa87be06. This affects the function customAxios of the file app/api/proxy/route.ts of the component Proxy API Endpoint. The manipulation of the argument url leads to server-side request forgery. The attack is possible to be carried out remotely. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	7.3	CVE-2026-19374
adaltas--backmeup	The backmeup npm package assembles shell command strings by directly concatenating its option values (name, source, destination, filter) - e.g. cmd = "mkdir -p " + path.join(info.destination, info.name) + "; " - and executes the resulting string through a shell via ssh2-exec (locally via child_process, or remotely via SSH when an ssh handle is supplied), rather than using execFile/spawn with an	2026-08-05	8.8	CVE-2026-71243

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	argument array. The only processing applied is path.normalize()/path.join(), which do not neutralize shell metacharacters (;, , &, \$(), backticks, newline). Any application that passes attacker-influenced values into these options (e.g. a user-chosen backup name) is vulnerable to arbitrary OS command execution on the backup host, or on the remote SSH target when one is configured.			
Admidio--admidio	Admidio before 5.0.11 contains an authentication bypass vulnerability in the forum module when configured in login-only mode. The access control logic in modules/forum.php fails to validate the login-only configuration state, allowing unauthenticated attackers to read forum topics and posts by directly accessing the module with read-only parameters.	2026-08-03	7.5	CVE-2026-69091
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements Used in a Template Engine vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-03	10	CVE-2026-48323
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary SQL commands, potentially gaining elevated access or control over the application. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-03	10	CVE-2026-48330
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in privilege escalation. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-03	10	CVE-2026-48331
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-03	9.6	CVE-2026-48317
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-03	9.9	CVE-2026-48326
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Incorrect Authorization vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain elevated privileges. Exploitation of this issue does not require user interaction.	2026-08-03	9.8	CVE-2026-48333
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by a Violation of Secure Design Principles vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction.	2026-08-03	7.5	CVE-2026-48399
advplyr--audiobookshelf	audiobookshelf's authentication-exemption check (server/routers/Auth.js) matches unauthenticated-allowed GET routes against req.path via a regex requiring a literal /items/:id/cover or /authors/:id/image shape, where req.path retains %2F sequences URL-encoded. Express's router decodes the :id route parameter before handler code runs, so a %2F-encoded './' sequence in :id (e.g. ../%2f..%2f..%2ftmp%2fpwned) passes the literal-path auth-exemption check while resolving to a real path-traversal payload once decoded. CacheManager.handleCoverCache then joins this decoded value into a cache file path and streams the result before any database-backed ownership check. This bypasses the fix applied for CVE-2025-25205 (which anchored the exemption regex and switched it to req.path) and results in unauthenticated arbitrary file read of any file matching the pattern *_{width}[x<height>].<ext> that the service account can read.	2026-08-05	7.5	CVE-2026-71209
AffiliateWP--AffiliateWP	Unauthenticated Cross Site Scripting (XSS) in AffiliateWP <= 2.35.0 versions.	2026-08-06	7.1	CVE-2026-65515
Aircoookie--WLED	WLED's GET /json/cfg endpoint (registered in wled00/wled_server.cpp) calls serveJson() with no settings-PIN check, unlike the /edit endpoint which explicitly checks correctPIN, disclosing the device's general configuration (network, hardware, LED setup) to any unauthenticated client on the network. Separately, the settings-PIN unlock state is tracked via a single global boolean 'correctPIN' (wled00/wled.h), not per-session state: once any single client submits the correct 4-digit PIN via POST /json, correctPIN becomes true for every client, granting all	2026-08-05	8.2	CVE-2026-71264

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	subsequent unauthenticated clients full configuration-write access (OTA firmware updates, WiFi reconfiguration, factory reset) until the device reboots.			
Amazon--Kiro CLI	An uncontrolled search path element in Kiro CLI before version 2.10.0 on Windows might allow a remote unauthenticated actor to execute arbitrary code via a maliciously crafted project directory containing an executable that bypasses workspace trust protections when a local user starts Kiro CLI in the directory. To remediate this issue, users should upgrade to version 2.10.0 or higher.	2026-08-04	7.8	CVE-2026-18657
Amazon--Kiro IDE	An uncontrolled search path element in Kiro IDE before version 1.0.228 on Windows might allow a remote unauthenticated actor to execute arbitrary code via a maliciously crafted project directory containing an executable that bypasses workspace trust protections when a local user opens the directory. To remediate this issue, users should upgrade to version 1.0.228 or higher.	2026-08-04	7.8	CVE-2026-18656
Amir Helzer--WooCommerce Multilingual & Multicurrency	Subscriber Cross Site Scripting (XSS) in WooCommerce Multilingual & Multicurrency <= 5.5.6 versions.	2026-08-06	7.1	CVE-2026-66711
AncoraThemes--Abogado	Unauthenticated PHP Object Injection in Abogado <= 1.18 versions.	2026-08-06	9.8	CVE-2026-65574
AncoraThemes--Accalia	Unauthenticated PHP Object Injection in Accalia <= 1.5.3 versions.	2026-08-06	9.8	CVE-2026-65575
AncoraThemes--Adrena	Unauthenticated PHP Object Injection in Adrena <= 1.2.14 versions.	2026-08-06	9.8	CVE-2026-65576
AncoraThemes--Advice	Unauthenticated PHP Object Injection in Advice <= 1.18.0 versions.	2026-08-06	9.8	CVE-2026-65577
AncoraThemes--Agora	Unauthenticated PHP Object Injection in Agora <= 1.9 versions.	2026-08-06	9.8	CVE-2026-65578
approve-me--Formidable Forms Signature Online Contract Automation	Unauthenticated Insecure Direct Object References (IDOR) in Formidable Forms Signature Online Contract Automation <= 2.0.1 versions.	2026-08-06	7.5	CVE-2026-65523
art-template--art-template	art-template's sub-template resolution logic (src/compile/adapters/resolve-filename.js), used by both the include() and extend() template directives, resolves the target file path via path.resolve(root, filename) with no check afterward that the result remains inside root. Because path.resolve() discards root entirely when filename is an absolute path, and does not block '../' traversal sequences, and the resolved path is passed directly to fs.readFileSync() in loader.js with its contents compiled and rendered, an application that lets a sub-template name be influenced by external input (e.g. a query parameter passed into {{include page}}) allows an attacker to read arbitrary files on disk that the Node process can access.	2026-08-05	7.5	CVE-2026-71215
ATN-B1--CPDLC	Lack of authentication for Very High Frequency Data Link messages allows rogue ground stations to inject CPDLC messages leading to unexpected or misleading clearances and potential pilot confusion. This type of attack can be carried out remotely over radio frequency.	2026-08-07	7.1	CVE-2025-71409
ATN-B1--CPDLC	Injection of false emergency or status messages over CPDLC may lead to misallocation of resources, operational confusion, and improper response actions by flight crews, traffic controllers, and ground operations. This type of attack can be carried out remotely over radio frequency.	2026-08-07	7.1	CVE-2025-71412
Autodesk--FBX SDK	A maliciously crafted FBX file, when parsed through Autodesk FBX SDK, can trigger a stack-based buffer overflow vulnerability in fbxsdk::FbxIO::BinaryReadSectionHeader. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	2026-08-04	7.8	CVE-2026-10709
Autodesk--FBX SDK	A maliciously crafted FBX file, when parsed through Autodesk FBX SDK, can trigger a stack-based buffer overflow vulnerability in fbxsdk::ExtractDrive. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	2026-08-04	7.8	CVE-2026-10710
Autodesk--Revit	A maliciously crafted PDF file, when parsed through Autodesk Revit, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	2026-08-06	7.8	CVE-2026-11803
Autodesk--Revit	A maliciously crafted PDF file, when parsed through Autodesk Revit, can force a Use-After-Free vulnerability. A malicious actor can leverage this vulnerability to cause a crash, disclose sensitive data, or execute arbitrary code in the context of the current process.	2026-08-06	7.8	CVE-2026-1289

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Autodesk--Revit	A maliciously crafted BMP file, when parsed through certain Autodesk products, can force a Untrusted Pointer Dereference vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	2026-08-06	7.8	CVE-2026-7406
Autodesk--Revit	A maliciously crafted PDF file, when parsed through Autodesk Revit, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	2026-08-06	7.8	CVE-2026-8325
AWS--Amazon Bedrock AgentCore harness	Insufficient input validation in Amazon Bedrock AgentCore harness might allow an authenticated remote user to execute configured tools bypassing model invocation and security controls via crafted content blocks in conversation messages. AWS has addressed this issue. No customer action is required.	2026-08-04	8.1	CVE-2026-18830
AWS--aws-transform-mcp-server	Improper limitation of a pathname to a restricted directory in the get_resource tool in Amazon awslabs.aws-transform-mcp-server 0.1.0 through 0.1.4 might allow a context-dependent actor to write arbitrary files outside the intended working directory via the savePath parameter. To remediate this issue, users should upgrade to version 0.1.5 or later.	2026-08-05	8.6	CVE-2026-18953
AWS--strands-agents-tools	A prompt injection vulnerability in the shell tool in Amazon Strands Agents Tools before 0.8.0 might allow remote actors to execute arbitrary operating system commands on the agent's host via a crafted prompt that sets the non_interactive parameter to true, bypassing the human consent gate. To remediate this issue, users should upgrade to version 0.8.0.	2026-08-03	8.8	CVE-2026-18733
AWS--strands-agents-tools	Insecure direct object reference in the mongodb_memory, elasticsearch_memory, and mem0_memory tools in Amazon Strands Agents Tools before 0.8.3 might allow remote authenticated users to access, modify, or delete memories belonging to other tenants by influencing the LLM to emit tool calls with a forged namespace parameter. To remediate this issue, users should upgrade to version 0.8.3.	2026-08-06	8.1	CVE-2026-19111
Axiomthemes--69 Clothing	Unauthenticated PHP Object Injection in 69 Clothing <= 1.2.11.1 versions.	2026-08-06	9.8	CVE-2026-65571
Axiomthemes--A.Williams	Unauthenticated PHP Object Injection in A.Williams <= 1.3.1 versions.	2026-08-06	9.8	CVE-2026-65572
axiomthemes--Agricola	Unauthenticated PHP Object Injection in Agricola <= 1.21.0 versions.	2026-08-06	9.8	CVE-2026-65579
Axiomthemes--AI ANN	Unauthenticated PHP Object Injection in AI ANN <= 1.29.0 versions.	2026-08-06	9.8	CVE-2026-65581
Ays Pro--Survey Maker	Unauthenticated Cross Site Scripting (XSS) in Survey Maker <= 5.2.3.3 versions.	2026-08-06	7.1	CVE-2026-65565
baserCMS Users Community--BaserCMS	BaserCMS provided by baserCMS Users Community contains a CSV file injection vulnerability. If a user downloads and opens a CSV file containing malicious code injected by an attacker, the malicious code may be executed.	2026-08-03	7.1	CVE-2026-65875
bensibley--Independent Analytics WordPress Analytics Plugin	The Independent Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 404 not_found_url tracking parameter in versions up to, and including, 2.15.0. This is due to the get_cell_content() function applying urldecode() after esc_url() when rendering the URL column for 404 entries - a sequence that allows percent-encoded HTML to pass URL validation and then be reconstructed as raw markup, which wp_kses_post() does not strip because it retains img elements and data-* attributes, and because the public REST endpoint /iawp/search accepts unauthenticated requests as long as they carry a signature that is itself embedded in public page HTML. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-05	7.2	CVE-2026-17506
BeRocket--Advanced AJAX Product Filters	Unauthenticated Cross Site Scripting (XSS) in Advanced AJAX Product Filters <= 3.2.0.3 versions.	2026-08-06	7.1	CVE-2026-66439
Bilin Software and Informatics Consultancy Inc.--HUMANIST Digital Human Resources	Unrestricted upload of file with dangerous type vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Upload a Web Shell to a Web Server. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	9.8	CVE-2026-14175
Bilin Software and Informatics Consultancy Inc.--HUMANIST Digital Human Resources	Use of hard-coded cryptographic key vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Read Sensitive Constants Within an Executable. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	9.1	CVE-2026-14804

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Bilin Software and Informatics Consultancy Inc.-- HUMANIST Digital Human Resources	Cleartext storage of sensitive information vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows SQL Injection. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	9.8	CVE-2026-15721
Bilin Software and Informatics Consultancy Inc.-- HUMANIST Digital Human Resources	Use of GET request method with sensitive query strings vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Session Hijacking. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	7.4	CVE-2026-14838
bitpressadmin--File Manager	The File Manager plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the connector function in all versions from 6.0 - 6.9. This makes it possible for authenticated attackers, with subscriber-level access and above, to read and delete arbitrary files on the server, which can lead to remote code execution when the right file is deleted (such as wp-config.php). The bypass is triggered by passing cmd=rm or cmf=file in the URL query string of a POST request: elFinder's bind registration reads the command exclusively from \$_POST and therefore never registers the rm.pre permission handler, while the dispatcher reads from the merged \$_GET+\$_POST superglobal and executes the rm or file command unchecked against a volume that defaults to ABSPATH.	2026-08-06	8.8	CVE-2026-15991
Bohdan Triapitsyn--OpenChamber	OpenChamber 1.11.7 contains an unauthenticated remote code execution vulnerability that allows remote attackers to execute arbitrary shell commands by sending crafted POST requests to the /api/fs/exec endpoint, which passes commands verbatim to Node.js spawn() without any allowlist, blocklist, or argument validation. The authentication middleware becomes a no-op when UI_PASSWORD is not configured, matching the default Docker deployment, enabling attackers to execute arbitrary OS commands as the application user and retrieve full command output including stdout, stderr, and exit code from the server response.	2026-08-06	9.8	CVE-2026-53975
Bohdan Triapitsyn--OpenChamber	OpenChamber 1.11.7 contains a path traversal vulnerability in the file-serving endpoints /api/fs/read, /api/fs/stat, and /api/fs/raw that allows unauthenticated remote attackers to read arbitrary files by supplying the allowOutsideWorkspace=true query parameter alongside an absolute path, bypassing the workspace boundary check in resolveReadPathFromContext. Attackers can exploit the vacuous isPathWithinRoot guard to read sensitive files such as the JWT signing secret, SSH private keys, API credentials, and environment variables, enabling full authentication bypass by forging session cookies on password-protected deployments.	2026-08-06	9.1	CVE-2026-53976
Bohdan Triapitsyn--OpenChamber	OpenChamber 1.11.7 contains an authentication bypass vulnerability that allows unauthenticated remote attackers to terminate the server process by sending a POST request to the /api/system/shutdown endpoint, which is registered before the authentication middleware in the Express route handler chain. Attackers can exploit the route registration order in bootstrap-runtime.js to reach the shutdown handler before auth middleware executes, causing denial of service to all active AI coding sessions and locking out legitimate remote users regardless of whether UI_PASSWORD is configured.	2026-08-06	7.5	CVE-2026-53977
BoldGrid--Total Upkeep	Unauthenticated Broken Access Control in Total Upkeep <= 1.17.2 versions.	2026-08-06	8.2	CVE-2026-66708
bolt--core	Bolt CMS renders content field values through Twig's full application-level Environment with no SandboxExtension registered anywhere in the codebase. In src/Entity/Field.php, getTwigValue() calls shouldBeRenderedAsTwig(), which gates rendering only on the field definition's allow_twig flag and a regex checking for '{{', '%', or '#'; when true, the raw field value is compiled and rendered via 'self::getTwig()->createTemplate(\$value)->render(['record' => \$this->getContent()])' with no sandboxing. Bolt's own bundled config/bolt/contenttypes.yaml sets 'allow_twig: true' on the default "pages" contenttype's content field out of the box. Any user with edit access to that content type (a standard editor role, not just an administrator) can inject a Twig payload such as '{{ [id] map('passthru') join }}' that executes arbitrary OS commands when the content is saved and rendered, achieving remote code execution as the web server user.	2026-08-05	8.8	CVE-2026-71291
boringproxy--boringproxy	boringproxy through 0.10.0 contains a newline injection vulnerability that allows authenticated low-privileged users with tunnel-creation permission to inject arbitrary lines into the server account's SSH authorized_keys file by supplying a	2026-08-05	9.9	CVE-2026-70615

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	percent-encoded newline character in the domain parameter of the tunnel creation endpoint. Attackers can insert an unrestricted public key entry into authorized_keys to gain persistent shell access, and subsequently read cleartext credentials from the database file including all user tokens, tunnel private keys, and TLS certificates.			
Brandexponents--Type Hub	Unauthenticated Arbitrary File Upload in Type Hub <= 2.0.6 versions.	2026-08-06	10	CVE-2026-66665
brix--crypto-js	crypto-js is a JavaScript library of crypto standards. Versions of crypto-js prior to 4.0.0 generate randomness in CryptoJS.lib.WordArray.random() using a custom variation of the Multiply-With-Carry pseudorandom number generator, seeded from Math.random(), instead of a cryptographically secure source. This generator was introduced in version 3.1.2-4 and remained present in nearly every 3.x release. Nominal requests for 128 or 256 bits of entropy through this function produce effective search spaces of approximately 2 to the 39th and 2 to the 47th possibilities, small enough to enumerate on commodity hardware. Downstream wallet applications that used CryptoJS.lib.WordArray.random() as the entropy source for BIP39 recovery phrases are affected, and an attacker who enumerates the reduced output space can recover the resulting private keys and control the associated funds. This issue is fixed in version 4.0.0.	2026-08-07	9	CVE-2026-71851
Cacti--cacti	Cacti's sanitize_sql_column() (lib/functions.php) sanitizes user-supplied ORDER BY column names using the regex `preg_replace('/[^a-zA-Z0-9_().]/', '', \$column)`. Because this allowlist retains letters, digits, underscore, parentheses, and dot (intended to support expressions like COUNT(id) and table.column), a payload such as `SLEEP(5)` passes through completely unmodified. The sanitized value is concatenated directly into raw SQL ORDER BY clauses (which cannot be parameterized) driven by a `sort_column` GET parameter in at least user_log.php, utilities.php, user_domains.php, and user_group_admin.php, allowing any authenticated Cacti user, regardless of privilege level, to perform time-based blind SQL injection against the Cacti database.	2026-08-05	8.8	CVE-2026-71287
CheckMAL--AppCheck Pro	A security flaw has been discovered in CheckMAL AppCheck Pro 3.1.43.10. Affected is an unknown function in the library AppCheckD.sys of the component Kernel Mini-Filter Driver. Performing a manipulation results in uncontrolled search path. The attack requires a local approach. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	7	CVE-2026-18605
chiuwingyan--house	A vulnerability has been found in chiuwingyan house up to dea6bceaebe2b364a5a209747f48ecc2b2dc670. This affects an unknown part of the file /paid/selectall.action. The manipulation of the argument zuname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	7.3	CVE-2026-19062
Cinnamon--kotaemon	kotaemon through 0.12.0 contains an insecure deserialization vulnerability in the check_connection endpoint that allows unauthenticated attackers to instantiate arbitrary Python classes by supplying crafted YAML/JSON input with a __type__ field. Attackers can exploit this to override the __type__ field with subprocess.check_output and arbitrary arguments, achieving remote code execution with application process privileges.	2026-08-04	9.8	CVE-2026-69098
Cisco--Cisco Catalyst SD-WAN Controller	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Catalyst SD-WAN engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20303 are related to improper input validation issues that are grouped under the Common Weakness Enumeration (CWE) CWE-20.	2026-08-05	9.9	CVE-2026-20303
Cisco--Cisco Catalyst SD-WAN Controller	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Catalyst SD-WAN engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20304 are related to improper access control issues that are grouped under the Common Weakness Enumeration (CWE) CWE-284.	2026-08-05	9.9	CVE-2026-20304

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco Catalyst SD-WAN Controller	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Catalyst SD-WAN engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20310 are related to improper link resolution before file access issues that are grouped under the Common Weakness Enumeration (CWE) CWE-59.	2026-08-05	9.1	CVE-2026-20310
Cisco--Cisco Catalyst SD-WAN Controller	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Catalyst SD-WAN engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20312 are related to Cleartext storage of sensitive information issues that are grouped under the Common Weakness Enumeration (CWE) CWE-312.	2026-08-05	8.8	CVE-2026-20312
Cisco--Cisco Catalyst SD-WAN Controller	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Catalyst SD-WAN engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20313 are related to Improper link resolution before file access issues that are grouped under the Common Weakness Enumeration (CWE) CWE-1284.	2026-08-05	7.7	CVE-2026-20313
Cisco--Cisco IOS XE Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XE Software engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20267 are related to improper access control issues that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-284.	2026-08-05	9	CVE-2026-20267
Cisco--Cisco IOS XE Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XE Software engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20272 are related to issues with improper neutralization of special elements that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-74.	2026-08-05	9.8	CVE-2026-20272
Cisco--Cisco IOS XE Software	A vulnerability in the Blocks Extensible Exchange Protocol (BEEP) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling when parsing a specific BEEP SOAP request. An attacker could exploit this vulnerability by sending a specific BEEP SOAP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.	2026-08-05	8.6	CVE-2026-20263
Cisco--Cisco IOS XE Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XE Software engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20268 are related to issues with improper restriction of operations within the bounds of a memory buffer that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-119.	2026-08-05	8.6	CVE-2026-20268
Cisco--Cisco IOS XE Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XE Software engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20269 are related to issues with improper control of a resource through its lifetime that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-664.	2026-08-05	8.6	CVE-2026-20269
Cisco--Cisco IOS XE Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XE Software engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20270 are related to incorrect calculation issues that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-682.	2026-08-05	8.6	CVE-2026-20270
Cisco--Cisco IOS XE Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XE Software engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20271 are related to insufficient control flow management issues that	2026-08-05	8.6	CVE-2026-20271

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-691. 			
Cisco--Cisco IOS XE Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco IOS XE Software engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20273 are related to improper input validation issues that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-20.	2026-08-05	8.6	CVE-2026-20273
Cisco--Cisco IOS XE Software	A vulnerability in the Extensible Messaging Client Protocol (XMCP), also referred to as the External Client protocol, of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of malformed XMCP packets. An attacker could exploit this vulnerability by sending a malformed XMCP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload unexpectedly, resulting in a DoS condition. The attacker does not need the XMCP client username to exploit this vulnerability.	2026-08-05	8.6	CVE-2026-20301
Cisco--Cisco IOS XE Software	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to improper error handling when parsing SNMP requests. This vulnerability affects all versions of SNMP -- Versions 1, 2c, and 3. An attacker could exploit this vulnerability by sending a malformed SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly. The attacker must have the SNMPv1 or v2c read-only or read-write community string or valid SNMPv3 user credentials on the affected device.	2026-08-05	7.7	CVE-2026-20124
Cisco--Cisco Secure Endpoint	A vulnerability in the zip archive parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to improper boundary checks for content in zip files during scanning, which may result in an out-of-bounds write condition. An attacker could exploit this vulnerability by submitting a crafted zip file for scanning. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-08-07	7.5	CVE-2026-20337
Cisco--Cisco Secure Endpoint	A vulnerability in the zip archive parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to improper memory handling when processing content in zip files during scanning. An attacker could exploit this vulnerability by submitting a crafted zip file for scanning. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate as a result of a memory double-free, resulting in a DoS condition on the affected software.	2026-08-07	7.5	CVE-2026-20338
Cisco--Cisco Secure Endpoint	A vulnerability in the PESpin file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition or possibly other expanded impacts as a result of memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in PESpin files during scanning, which may result in an integer overflow. An attacker could exploit this vulnerability by submitting a crafted file that contains PESpin content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-08-07	7.5	CVE-2026-20339
Cisco--Cisco Secure Endpoint	A vulnerability in the GPT file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition or possibly other expanded impacts as a result of memory corruption on an affected device. This vulnerability is due to improper handling of an endian conversion operation, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted GPT file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-08-07	7.5	CVE-2026-20345
Cisco--Cisco Secure Endpoint	A vulnerability in the PDF file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition or possibly other expanded impacts as a result of memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in PDF files during scanning, which may result in an out-of-bounds buffer read. An attacker	2026-08-07	7.5	CVE-2026-20346

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could exploit this vulnerability by submitting a crafted PDF file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.			
Cisco--Cisco Secure Endpoint	A vulnerability in the Mach-O file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition or possibly other expanded impacts as a result of memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in Mach-O files during scanning, which may result in an out-of-bounds buffer read. An attacker could exploit this vulnerability by submitting a crafted Mach-O file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-08-07	7.5	CVE-2026-20347
Cisco--Cisco Secure Endpoint	A vulnerability in the XAR file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition or possibly other expanded impacts as a result of memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in XAR files during scanning. An attacker could exploit this vulnerability by submitting a crafted file that contains XAR content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-08-07	7.5	CVE-2026-20348
Cisco--Cisco Unified Computing System (Standalone)	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with low privileges to execute arbitrary commands on the underlying operating system of an affected system and elevate privileges to root. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by entering crafted inputs to the web-based management interface of the affected software. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the root user.	2026-08-05	8.8	CVE-2026-20200
ClearFoundation--ClearOS	ClearOS 7.9 contains an OS command injection vulnerability in the Log Viewer component that allows authenticated attackers to execute arbitrary commands by submitting unsanitized input through the filter parameter, which is interpolated directly into a shell command in File.php. Attackers can inject command substitution payloads into the filter parameter to execute arbitrary commands as the webconfig user, and due to extensive NOPASSWD sudo privileges granted to that user by default, immediately escalate to root.	2026-08-03	7.2	CVE-2026-67599
CoCart--CoCart	The CoCart WordPress plugin before 4.9.0 does not validate a user-supplied price value against the actual product price when items are added to the cart through one of its public REST API endpoints, allowing unauthenticated users to set arbitrary product prices and complete WooCommerce orders at manipulated totals.	2026-08-06	7.5	CVE-2026-10524
code-projects--Task Management System	A vulnerability was detected in code-projects Task Management System 1.0. Affected is an unknown function of the file /index.php of the component Login. Performing a manipulation of the argument Password results in improper authentication. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2026-08-09	7.3	CVE-2026-19342
code-projects--Task Management System	A flaw has been found in code-projects Task Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/AdminLogin.php. Executing a manipulation of the argument email/password can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	2026-08-09	7.3	CVE-2026-19343
code-projects--Task Management System	A vulnerability has been found in code-projects Task Management System 1.0. Affected by this issue is some unknown functionality of the file /user/comment_count_user.php. The manipulation of the argument task_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2026-08-09	7.3	CVE-2026-19344
Constant Contact--Creative Mail	Subscriber SQL Injection in Creative Mail <= 1.6.9 versions.	2026-08-06	8.5	CVE-2026-65547
Contiki-NG--Contiki-NG	Contiki-NG's MQTT client parse_publish_vhdr() in os/net/app-layer/mqtt/mqtt.c sets topic_len_received=1 before checking topic_len against the 64-byte limit, so an over-length topic returns early but leaves the flag set. On the next TCP segment, tcp_input() re-invokes the parser with topic_received==0, and the persisted topic_len_received==1 skips the length-reading block containing the guard, falling through directly to a memcpy() that uses the unvalidated 16-bit topic_len as the	2026-08-06	8.1	CVE-2026-5857

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	copy length. The 65-byte topic[] destination overruns into adjacent struct fields including the payload_chunk pointer, which subsequent MQTT code dereferences, giving a compromised or attacker-controlled broker an arbitrary-pointer-write primitive. Contiki-NG's MQTT implementation has no TLS support so the connection is plaintext. Impact ranges from information disclosure and denial of service to remote code execution on embedded targets without memory protection.			
Contiki-NG-- Contiki-NG	Contiki-NG's LwM2M TLV parser lwm2m_tlv_read() in os/services/lwm2m/lwm2m-tlv.c ignores its caller-supplied buffer length argument and reads up to six bytes from the input buffer with no bounds check. The caller in lwm2m-engine.c iterates while there is at least one byte remaining, so a crafted CoAP WRITE to any LwM2M endpoint whose final TLV supplies exactly one byte triggers up to five out-of-bounds reads of heap memory adjacent to the CoAP input buffer, disclosing memory contents (including key material and peer addresses) through the parsed tlv->id, tlv->length, and tlv->value fields. Corrupted tlv_len derived from the out-of-bounds memory further corrupts the caller's parse offset. In LwM2M NoSec mode, the default for constrained devices, no authentication is required.	2026-08-06	7.5	CVE-2026-5855
Contiki-NG-- Contiki-NG	Contiki-NG's DNS/mDNS resolver skip_name() in os/services/resolv/resolv.c walks DNS wire-format name labels with no packet-boundary check, and the caller in newdata() invokes it in a loop iterating nquestions times from the attacker-controlled DNS header before validating the transaction ID. An attacker who sets nquestions higher than the number of complete questions present causes skip_name() to walk past the UDP packet buffer, and the returned pointer is cast to struct dns_answer * for further memory reads. On builds with RESOLV_CONF_SUPPORTS_MDNS enabled, any peer on the local segment can trigger the read unauthenticated via a multicast UDP 5353 packet with no outstanding query required; on standard DNS builds an attacker who can inject a UDP response from port 53 during an outstanding query can trigger the same read. Impact is out-of-bounds read of uip_buf and adjacent memory, disclosing memory contents or crashing the resolver.	2026-08-06	7.1	CVE-2026-5856
cornelraiu-1-- Search Analytics for WP	The Search Analytics for WP plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.16. This is due to missing or incorrect nonce validation on the `process_bulk_action()` function of `MWTSA_Stats_Table`. This makes it possible for unauthenticated attackers to delete arbitrary search-term records, including all associated search-history rows, via a forged request granted they can trick a user with access to the plugin's "Search Analytics" dashboard page (Administrator by default) into performing an action such as clicking on a link.	2026-08-05	8.1	CVE-2026-7444
Cotonti--Cotonti	Cotonti CMS's Comments plugin deserializes user-supplied data without restricting the classes that may be instantiated. In plugins/comments/controllers/actions/CreateAction.php, a `ci` POST parameter obtained via `cot_import('ci', 'P', 'TXT')` (trim-only sanitization) is passed to `unserialize(base64_decode(\$ci))` with no `allowed_classes` restriction, reachable by any member with write access to comments (the default `Auth_members => 'RW'` setting in plugins/comments/comments.setup.php). In plugins/comments/controllers/actions/EditAction.php, a `cb` parameter is similarly deserialized via `unserialize(base64_decode(\$this->comeback))` in prepareComeBack(), reachable by any member editing their own comment. Because unserialize() is called without allowed_classes, an attacker can construct a serialized PHP object of any class loaded by Cotonti (a PHP Object Injection primitive). This was demonstrated in practice using Cotonti's own MySQL_cache class: a crafted serialized MySQL_cache object, once deserialized and later garbage-collected, triggers its __destruct()->flush() chain, causing an attacker-controlled INSERT INTO cot_cache with attacker-chosen row values - confirming genuine POP-chain exploitation, with further impact (including potential RCE) contingent on other gadget chains available in a given Cotonti installation's loaded classes. A third sink in DeleteAction.php contains the identical unserialize() pattern but is gated behind an admin-only authorization check and is not reachable by ordinary members.	2026-08-05	7.7	CVE-2026-71294
cozmoslabs-- TranslatePress Translate Multilingual sites with AI Translation	The TranslatePress - Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content (URL-encoded gettext markers) in all versions up to, and including, 3.2.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Comment moderation may delay	2026-08-06	7.2	CVE-2026-18510

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation for first-time commenters, but does not prevent it, as the payload uses only WordPress-permitted tags and attributes with percent-encoded characters that pass wp_kses URL validation unmodified.			
crater-invoice--Crater	Crater isolates data per company_id, and its Invoice/Estimate/Payment/Expense policies enforce both a Bouncer ability check and \$user->hasCompany(\$model->company_id). CustomerPolicy's view/update/delete methods omit the company-ownership check entirely, checking only the blanket ability. Route-model-bound customer lookups and the bulk Customer::deleteCustomers() method are similarly unscoped (self::find(\$id) with no company filter). Any authenticated user of one company can read, reassign (steal), or delete another company's customer records, with deletion cascading to that customer's invoices and payments.	2026-08-05	8.2	CVE-2026-55739
crater-invoice--crater	Crater's NotePolicy checks only a blanket Bouncer ability (manage-all-notes / view-all-notes) with no company-ownership comparison, unlike InvoicePolicy and other sibling policies which additionally verify \$user->hasCompany(\$model->company_id). NotesController's show(), update(), and destroy() actions authorize via \$this->authorize('view notes'/'manage notes') without passing the target Note model, and Note's company-scoping (scopeWhereCompany) is applied only in the list endpoint, not in show/update/destroy. Any authenticated user of one company can read, edit, or delete another company's notes by ID. This is a distinct finding from the previously reported CustomerPolicy company-ownership omission (a different policy class and controller).	2026-08-05	8.2	CVE-2026-71242
Creative Mail--Creative Mail	The Creative Mail WordPress plugin from 1.6.5 to 1.6.9 does not sanitize and escape a parameter before using in an SQL statement, leading to an unauthenticated SQL injection when the abandoned cart email is managed by creative mail.	2026-08-06	8.6	CVE-2026-3430
Crocoblock. Jetimpex Inc.--JetEngine	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.13.1 versions.	2026-08-06	7.1	CVE-2026-28082
cwalter-at--FreeModbus	The LINUXTCP port of FreeModbus contains an off-by-one bounds check in xMBPortTCPPool() (demo/LINUXTCP/port/porttcp.c). The check `if (usTCPFrameBytesLeft > MB_TCP_BUF_SIZE)` uses a strict greater-than comparison instead of greater-than-or-equal against the 263-byte MB_TCP_BUF_SIZE limit. An MBAP frame with a Length field of 264 makes usTCPFrameBytesLeft equal to 263, which passes the flawed check, and the subsequent recv() call writes up to 263 bytes starting at buffer offset 7 into the 263-byte static buffer aucTCPBuf, overflowing it by 7 bytes into the adjacent static variable usTCPBufPos. A single crafted, unauthenticated Modbus TCP packet triggers the overflow, since Modbus has no built-in authentication.	2026-08-05	9.1	CVE-2026-71263
cyberlord92--Page and Post Restriction	The Page and Post Restriction plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to and including 1.4.0 via the WordPress core REST endpoints /wp-json/wp/v2/pages, /wp-json/wp/v2/pages/<id>, /wp-json/wp/v2/posts, and /wp-json/wp/v2/posts/<id>. This is due to the plugin's REST guards - papr_restrict_page_post_rest_api() and the the_posts filter registered by papr_filter_posts() - sourcing their restricted-ID list exclusively from papr_get_restricted_posts_id(), which only reads the per-page metabox options papr_allowed_redirect_for_pages and papr_allowed_redirect_for_posts and never consults the two global toggles papr_access_for_only_loggedin and papr_access_for_only_loggedin_posts that the plugin's own UI describes as 'Make all Pages Private' / 'Make all Posts Private'. This makes it possible for unauthenticated attackers to read the full rendered content of every published page and post on sites configured with the documented global toggles, bypassing the security boundary enforced on the frontend by papr_restrict_logged_in_users().	2026-08-05	7.5	CVE-2026-12000
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formLtefotaUpgradeQuectel interface. A remote attacker can inject arbitrary malicious commands into the fota_url field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71944
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formLtefotaUpgradeFibocom interface. A remote attacker can inject arbitrary malicious commands into the fota_url field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71945

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formPingDiagnosticRun interface. A remote attacker can inject arbitrary malicious commands into the host field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71946
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formTracerouteDiagnosticRun interface. A remote attacker can inject arbitrary malicious commands into the host and ipVer fields, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71947
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formDebugDiagnosticRun interface. A remote attacker can inject arbitrary malicious commands into the host field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71948
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formUSSDSetup interface. A remote attacker can inject arbitrary malicious commands into the ussdValue and selectMenuValue fields, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71949
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formSmsManage interface. A remote attacker can inject arbitrary malicious commands into the action_value field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71950
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formIMEISetup interface. A remote attacker can inject arbitrary malicious commands into the IMEI_value field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71951
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formPinManageSetup interface. A remote attacker can inject arbitrary malicious commands into the oldPin field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71952
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formNtp interface. A remote attacker can inject arbitrary malicious commands into the ntpServerIp1 field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71953
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and firmware version before 1.1.5_C1_202607071108 contain a command injection vulnerability in the /boafrm/formL2tpv3ConfigSetup interface. A remote attacker can inject arbitrary malicious commands into the tunnelid and sessionid fields, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71954
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and software version 1.1.2_C1_202602110044 contain a command injection vulnerability in the /boafrm/formWsc interface. A remote attacker can inject arbitrary malicious commands into the localPin, targetAPSid, peerPin, and peerRptPin fields, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71955
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and software version 1.1.2_C1_202602110044 contain a command injection vulnerability in the app.cgi interface. A remote attacker can inject arbitrary malicious commands into the netDig.ping.dst field, resulting in command execution with root privileges.	2026-08-08	9.8	CVE-2026-71956
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and software version 1.1.2_C1_202602110044 contain a buffer overflow vulnerability in the app.cgi interface. A remote attacker can write an overly long string to the netAcc.addlist[].name field and execute arbitrary commands by crafting a specific payload, or cause the device to crash.	2026-08-08	9.8	CVE-2026-71957
D-Link Corporation--DWR-M961	D-Link DWR-M961 devices with hardware version C1 and software version 1.1.2_C1_202602110044 contain a buffer overflow vulnerability in the quicksetup.cgi interface. A remote attacker can write overly long strings to the test4, ssid2, and username fields and execute arbitrary commands by crafting a specific payload, or cause the device to crash.	2026-08-08	9.8	CVE-2026-71958

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Daniel Iser--Popup Maker	Unauthenticated Cross Site Scripting (XSS) in Popup Maker <= 1.23.0 versions.	2026-08-06	7.1	CVE-2026-28177
Data443 Risk Mitigation, Inc.--Tracking Code Manager	Unauthenticated Cross Site Request Forgery (CSRF) in Tracking Code Manager <= 2.6.0 versions.	2026-08-06	7.1	CVE-2026-28172
DataLinkDC--Dinky	Dinky's POST /download/uploadFromRsByLocal handler passes the caller-supplied path parameter directly to new File(path) and file.transferTo(dest) with no path validation. The route is marked @Salgnore and /download/** is excluded from the Sa-Token interceptor, so the only guard is a header equality check against a dinkyToken value whose default (efda1551-7958-4e0f-80a8-dfd107df3e38) is hardcoded in source and shipped to every deployment. Anyone who can reach Dinky's HTTP port (8888 by default) and supplies the hardcoded token can write arbitrary files as the Dinky service account. The default Docker image runs on 8888 with no proxy or authentication and chmod 777 on /opt/dinky, so the application's own classpath, launch scripts, and static assets are writable. Demonstrated impact: overwriting /opt/dinky/config/static/index.html served attacker JavaScript to admin browsers immediately, and writing /opt/dinky/org/dinky/Dinky.class executed attacker code as the Dinky service account at the next JVM start via a classpath-shadow launched by script/bin/auto.sh. Writes are uid 9999 (flink), not root, so /etc, /root, /home, and /usr are refused. Affects Dinky v1.2.5 (the current release) and the development branch, where the code is byte-identical.	2026-08-06	9.8	CVE-2026-70558
DataLinkDC--Dinky	Dinky's SysConfigController.getAll() handler for GET /api/sysConfig/getAll carries a method-level @Salgnore annotation that short-circuits the class-level @SaCheckLogin, so the Sa-Token interceptor lets the request through with no session or role check. Any remote unauthenticated caller who can reach the Dinky HTTP port (8888 by default) receives the full live system configuration (54 entries on a stock v1.2.5 install) with one parameterless GET. Only one credential field (sys.maven.settings.repositoryPassword) has a desensitization handler wired; the other credential-bearing fields (sys.env.settings.dinkyToken, sys ldap.settings.userPassword, sys.resource.settings.oss.accessKey and secretKey, and sys.dolphinscheduler.settings.token) return in cleartext. A bare install leaks the shipped defaults, including the hardcoded dinkyToken efda1551-7958-4e0f-80a8-dfd107df3e38 and minioadmin/minioadmin OSS keys; once an operator configures LDAP, object storage, or DolphinScheduler through the Settings Center, those live third-party credentials leak from the same endpoint. Because dinkyToken is the sole gate on the sibling POST /download/uploadFromRsByLocal arbitrary file write, this disclosure defeats token rotation as a mitigation for that vulnerability. Affects Dinky v1.2.5 (the current release, 2025-11-05) and the development branch (dev HEAD 63b5a5a), where the affected code is byte-identical.	2026-08-06	7.5	CVE-2026-70559
David Lingren--Media Library Assistant	Unauthenticated Cross Site Scripting (XSS) in Media Library Assistant <= 3.38 versions.	2026-08-06	7.1	CVE-2026-61963
debev--nanoMODBUS	nanoMODBUS through v1.23.0 contains an out-of-bounds write in the Modbus server-side handle_read_file_record() function (FC 0x14, Read File Record) in nanomodbus.c. The function validates that the total request size does not exceed 245 bytes and that each sub-request's record_length is at most 124, but it never validates the CUMULATIVE response size across all sub-requests before processing them. The accumulator response_data_size is declared as uint8_t and is incremented by 2 + record_length*2 for each of up to 35 sub-requests; with 35 sub-requests of record_length=124, the cumulative demand is 8750 bytes, which overflows the uint8_t accumulator. A subsequent loop then calls get_n(), an internal function with no bounds checking, once per sub-request to obtain a pointer into the 260-byte msg.buf receive buffer and advances the internal buf_idx by up to 248 bytes per call; swap_regs() then writes to that pointer unconditionally. A single crafted FC 0x14 request from an unauthenticated network client can cause up to ~8490 bytes to be written out of bounds past the 260-byte buffer, corrupting adjacent memory in the server process and leading to denial of service or potential remote code execution, particularly on embedded/bare-metal targets without memory protection.	2026-08-05	9.8	CVE-2026-71254
debev--nanoMODBUS	nanoMODBUS through v1.23.0 contains an out-of-bounds stack read leading to a wild-pointer write in nmbs_read_device_identification_basic() / recv_read_device_identification_res() in nanomodbus.c. A fixed 3-element stack array order[3] = {0,1,2} maps object IDs to buffer indices. The server-supplied	2026-08-05	9.8	CVE-2026-71256

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	object_id field (0-255, read directly from the wire) is used without any bounds check as buf_index = order[object_id]. When a malicious Modbus server sends a Read Device Identification response with object_id >= 3, this reads an out-of-bounds/garbage byte from the stack adjacent to order[], which is then used as an index into a 3-element buffers[] array of char* pointers. The resulting wild pointer is passed to strncpy() as the destination, causing an arbitrary-address write with server-controlled data.			
debev-- nanoMODBUS	nanoMODBUS through v1.23.0 contains an out-of-bounds write in the Modbus client-side recv_read_device_identification_res() function (FC 0x2B/MEI 0x0E, Read Device Identification) in nanomodbus.c. The server-supplied object_length field (0-246) is validated only against the remaining PDU size (res_size_left) and is never validated against the caller-supplied buffers_length parameter. After copying data with strncpy(buffers_out[buf_index], str, buffers_length), the code unconditionally writes a NUL terminator at buffers_out[buf_index][object_length]. When a malicious or compromised Modbus server sends a response with object_length greater than or equal to the client's buffers_length, this NUL write lands past the end of the caller-provided buffer, corrupting adjacent stack or heap memory on the client.	2026-08-05	8.6	CVE-2026-71255
decidim--decidim	Decidim is a participatory democracy framework. Prior to 0.31.5 and in 0.32.0.rc1 before 0.32.0.rc2, JWT-backed API authentication is not bound to the organization selected by the current host, allowing a JWT issued for one tenant to be replayed against another tenant's API to read participantDetails data and reach the proposal.answer mutation path. This issue is fixed in versions 0.31.5 and 0.32.0.rc2.	2026-08-06	8.5	CVE-2026-45414
decidim--decidim	Decidim is a participatory democracy framework. Prior to 0.30.9, from 0.31.0 before 0.31.5, and in 0.32.0.rc1 before 0.32.0.rc2, the identity-document verification admin UI embeds verification_attachment blobs through reusable signed Active Storage disk URLs, allowing anyone who obtains a URL to download the scanned document without an authenticated Decidim session until the signature expires. Verification-document images are rendered with variant_url(...), which produces signed /rails/active_storage/disk/... links instead of routing the file through an authorization-checking controller. Because Decidim configures Active Storage service URLs to remain valid for seven days, the URL itself becomes the credential for that period. The affected files are verification_attachment blobs on Decidim::Authorization, and the admin review pages embed those signed URLs directly into the HTML for pending and confirmation views. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.	2026-08-06	7.5	CVE-2026-45378
DeepCool-- DisplayService	A vulnerability was detected in DeepCool DisplayService 1.2.12. This issue affects some unknown processing of the file C:\DeepCool\resources\service\x64\DeepCoolDisplayService.exe. Performing a manipulation results in improper access controls. The attack must be initiated from a local position. The exploit is now public and may be used.	2026-08-07	7.8	CVE-2026-19192
Dell--Display and Peripheral Manager (DDPM Mac)	Dell Display and Peripheral Manager (DDPM Mac), versions prior to 2.3.0.1005, contain an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges and arbitrary code execution.	2026-08-03	7.8	CVE-2026-59912
Dell--Display and Peripheral Manager (DDPM Mac)	Dell Display and Peripheral Manager (DDPM Mac), versions prior to 2.3.0.1005, contain a Missing Authentication for Critical Function vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-08-03	7.8	CVE-2026-59913
Dell--OpenManage Server Administrator Managed Node (Patch) for Windows	Dell OpenManage Server Administrator, versions prior to 11.1.0.2, contains an Improper Authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-08-07	7.7	CVE-2026-56793
Dell--Virtual Storage Integrator for VMware vSphere Client	Dell Virtual Storage Integrator for VMware vSphere Client, versions prior to 10.11.1.0, contain(s) a Sensitive Information Disclosure vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to information disclosure and session hijacking. This vulnerability is considered critical as it allows an unauthenticated attacker to obtain active session credentials and fully impersonate authenticated users, including administrators. Dell recommends customers to upgrade at the earliest opportunity.	2026-08-06	9.1	CVE-2026-54489
Dell--Virtual Storage Integrator	Dell Virtual Storage Integrator for VMware vSphere Client, versions prior to 10.11.1.0, contain(s) an OS Command Injection vulnerability in the IAPI	2026-08-06	9.8	CVE-2026-67261

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
for VMware vSphere Client	component. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying operating system with root privileges. Exploitation may lead to a complete system takeover by an attacker. This vulnerability is considered critical as it allows an unauthenticated remote attacker to achieve arbitrary code execution as root, potentially compromising the entire VSI deployment and underlying infrastructure. Dell recommends customers to upgrade at the earliest opportunity.			
devitemslc--ShopLentor All-in-One WooCommerce Growth & Store Enhancement Plugin	The ShopLentor plugin for WordPress is vulnerable to arbitrary function execution via the woollentoropt/v1/custom-action REST API endpoint in all versions up to, and including, 3.3.7. This is due to the handle_action() method passing user-supplied input directly to call_user_func() without an allowlist of permitted callbacks. This makes it possible for authenticated attackers, with Administrator-level access and above, to execute arbitrary PHP callable functions via the 'callback' parameter.	2026-08-05	7.2	CVE-2026-6020
dgraph-io--dgraph	Dgraph is an open source distributed GraphQL database. Prior to 25.3.8, maybeQuoteArg in graphql/resolve/query_rewriter.go passes regexp filter strings into generated DQL without quoting or validating the /pattern/flags form, allowing crafted GraphQL query or mutation filters to inject DQL operators, disclose unintended nodes, or expand modification and deletion targets. This issue is fixed in version 25.3.8.	2026-08-06	8.6	CVE-2026-63637
dhax--go-base	go-base is a Go RESTful API Boilerplate template with JWT Authentication, backed by PostgreSQL. In versions prior to 2026-05-18, the JWT signing secret is hardcoded to the known string "random", letting any attacker who reads the public repository forge tokens for arbitrary users, including admin roles, and completely bypass authentication on all protected endpoints. This value is set in two places: the dev.env template (line 10) and a programmatic fallback in cmd/serve.go (line 35), so the application uses it even when no .env file is present. The original mitigation in auth/jwt/tokenauth.go (lines 22 to 25) only caught the exact string "random", letting other weak secrets through, and replaced it with an in-memory key that was not persisted, invalidating all tokens on every restart and effectively causing a denial-of-service. This issue has been fixed in version 2026-05-18.	2026-08-03	9.1	CVE-2026-48031
DjangoCRM--django-crm	DjangoCRM ships with its Django SECRET_KEY hardcoded directly in the committed webcrm/settings.py rather than read from an environment variable. Since this key is used for session signing, CSRF token generation, and password reset tokens, anyone who reads the public repository can forge valid session cookies (including for the superadmin account), forge CSRF tokens, and forge password reset tokens, achieving full account takeover. The repository also ships with DEBUG=True as the default, causing error pages to leak database credentials, email credentials, OAuth data, and internal file paths.	2026-08-05	9.1	CVE-2026-71238
DjangoCRM--django-crm	DjangoCRM's massmail module renders user-controlled EmlMessage fields (subject, content) through Django's Template() constructor with no sanitization, in at least three locations: message_previews.py builds an f-string embedding message.subject/message.content directly into a Template() call; email_creators.py passes eml_message.subject directly as a template string to Template(); and helpers.py contains the same f-string interpolation pattern. An authenticated user with mass-mail message edit rights can inject Django template syntax ({{ }} / {% %}) that executes at render time, enabling disclosure of other users' data and password hashes via request context variables, CSRF token forgery, and inclusion of arbitrary registered templates.	2026-08-05	8.1	CVE-2026-71239
djangoproject--Django	An issue was discovered in Django 5.2 before 5.2.17 and 6.0 before 6.0.8. GeoDjango spatial lookups optimistically parse the right-hand-side value as a raster by passing it to the `django.contrib.gis.gdal.GDALRaster` constructor. Any value used in a spatial lookup against a `GeometryField` or `RasterField` reaches this constructor, including untrusted input, for example a spatial-field filter submitted through the Django admin changelist query string by a staff user with view permission. A `dict`, or a `str` holding its JSON representation, is opened in write mode regardless of the constructor's `write=False` default, allowing a file with an attacker-chosen name and contents to be written through a file-backed GDAL driver. Any other `str` is treated as a datasource, allowing an outbound network request through a GDAL virtual filesystem handler. Writing a file to a location later imported by the application can result in remote code execution. Earlier, unsupported Django series (such as 5.1.x, 5.0.x, and 4.2.x) were not evaluated and	2026-08-04	8.8	CVE-2026-15307

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	may also be affected. Django would like to thank Bence Nagy, localhost-detect, and kimchunbok_ for reporting this issue.			
documize--community	Documize Community's attachment download route (domain/attachment/endpoint.go, Download function, registered via AddPublic with no auth middleware) accepts a `secure` query parameter and grants access whenever the parameter is simply non-empty (len(secureToken) > 0), without comparing it to any server-stored value. Any non-empty string, such as ?secure=x, bypasses authentication entirely and allows downloading any organization's attachments. Sibling handlers in the same file (togglePublish, delete) correctly enforce session-based authorization, confirming this is an inconsistency rather than intended design.	2026-08-05	7.5	CVE-2026-71234
dokaninc--Dokan: AI Powered WooCommerce Multivendor Marketplace Solution Build Your Own Amazon, eBay, Etsy	The Dokan plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 5.0.1. This is due to a missing authorization check in the `CustomersController` REST controller (`includes/REST/CustomersController.php`), which re-registers WooCommerce's customer CRUD routes under the `/dokan/v1/customers/` namespace and replaces WooCommerce's native `manage_woocommerce` capability check with a vendor-only check that inspects the `**requesting**` user's role and never validates the `**target**` user. This makes it possible for authenticated attackers with Vendor/Seller-level access and above to read, modify, or delete any WordPress user - including administrators - via `GET`/`PUT`/`DELETE` requests against `/wp-json/dokan/v1/customers/{id}`. Setting the `password` parameter on an administrator's record yields a full site takeover.	2026-08-05	8.8	CVE-2026-8761
domoticz--domoticz	Domoticz's MochadTCP::MatchLine() handler for MOCHAD_RFSEC messages (hardware/MochadTCP.cpp) copies network-received data from the up-to-1028-byte m_mochadbuffer into a fixed 50-byte stack buffer tempRFSECbuf using strcpy() with no length check, across three separate code branches (DS10A/KR10A/MS10A device types). An attacker on the local network segment able to reach the Mochad TCP bridge (default port 1099, no authentication) can send a crafted packet that overflows tempRFSECbuf by up to several hundred bytes, corrupting the Domoticz worker thread's stack.	2026-08-05	7.5	CVE-2026-71265
dresende--node-sql-query	A vulnerability was found in dresende node-sql-query 0.1.25/0.1.26/0.1.27/0.1.28. Affected by this vulnerability is the function SelectQuery.from/SelectQuery.build in the library lib/Select.js of the component Request Parameter Handler. Performing a manipulation results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. Upgrading to version 0.1.29 addresses this issue. The patch is named 3414c42f6de89826fa1f5f36f6139d1e6552778e. Upgrading the affected component is recommended.	2026-08-09	7.3	CVE-2026-19351
dromara--lamp-cloud	LAMP Rapid Development Platform through 5.6.2, fixed in commit 84b0c27, contains a remote code execution vulnerability in GlueFactory that executes unsandboxed Groovy scripts from database template fields without compilation restrictions or whitelisting. Attackers can write or influence the script field via message template endpoints to execute arbitrary Groovy code and OS commands on the backend server.	2026-08-04	8.8	CVE-2026-69100
E2Pdf--e2pdf	Unauthenticated Local File Inclusion in e2pdf <= 1.32.40 versions.	2026-08-06	8.1	CVE-2026-66710
e4jvikwp--VikAppointments Services Booking Calendar	VikAppointments Service Booking Calendar wordpress plugin is vulnerable to unauthenticated SQL injection due to one of the parameters that controls how the public reviews list is sorted is taken from the incoming request and used to build a database query without proper validation or sanitization. Because this value is placed directly into the query, an attacker who is not logged in can inject arbitrary SQL through a normal booking page and read data from the site's database - including sensitive information such as WordPress user credentials. No authentication or special privileges are required	2026-08-05	7.5	CVE-2026-15918
e4jvikwp--VikRentItems Flexible Rental Management System	The VikRentItems - Flexible Rental Management System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the customer email field of the booking checkout form in versions up to, and including, 1.2.1. This is due to insufficient input sanitization and output escaping in the saveorder() function, which stores the raw email value via VikRequest::getString() (applying only sanitize_text_field(), which does not neutralize HTML attribute-breaking characters such as double quotes), and in the editororder template which echoes the stored custmail value into an HTML input element's value attribute without esc_attr(). This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-05	7.2	CVE-2026-16143

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Eclipse Foundation-- Eclipse GlassFish	In Eclipse GlassFish versions 8.0.x before 8.0.4, CSRF + SSRF in DownloadServlet ContentSources leaks the admin `gfresttoken` to attacker-controlled host if the victim is authenticated into the Admin Console -> full unauthenticated takeover of Eclipse GlassFish domain until the token expires.	2026-08-06	9.6	CVE-2026-12605
Eclipse Foundation-- Eclipse Theia	In Eclipse Theia versions up to and including 1.73.1, the `@theia/filesystem` backend binds `POST /file-upload` in every filesystem-enabled deployment. The handler takes an attacker-supplied absolute path from the multipart `uri` field and calls `fs.move(tmp, target, { overwrite: true })` with no workspace confinement and no authentication. In browser (non-Electron) deployments the connection token is enforced only on WebSocket upgrades; the HTTP middleware in `@theia/core` re-issues the cookie and calls `next()` without rejecting tokenless HTTP requests. Because `multipart/form-data` is a CORS-safelisted request type, a cross-origin web page can trigger the write with no preflight and no credentials, resulting in an unauthenticated arbitrary file write outside the workspace to any absolute path the backend process can write. This can escalate to remote code execution, for example by overwriting a startup-executed file such as `~/bashrc`. Electron mode uses a separate `ElectronSecurityToken` and is not affected via this path.	2026-08-05	8.8	CVE-2026-60009
Eclipse Foundation-- Eclipse Theia	In Eclipse Theia versions 1.66.0 and up until including 1.73.1, the `@theia/plugin-ext` backend exposes the `/hostedPlugin/:pluginId/:path(*)` HTTP endpoint, which resolves the requested file path with `path.resolve(localPath, filePath)` without verifying that the resolved path stays within the plugin's directory. An unauthenticated network attacker can send percent-encoded `../` sequences (`%2e%2e%2f`) that decode into the path parameter and escape the plugin directory, allowing arbitrary files readable by the Theia backend process to be retrieved. Plugin IDs are derived deterministically from a plugin's publisher and name, so built-in plugins serve as reliable anchors that require no prior knowledge of the target system.	2026-08-05	7.5	CVE-2026-12609
Eclipse Foundation-- Eclipse Theia	In Eclipse Theia versions up to and including 1.73.1, the `@theia/filesystem` backend exposes HTTP file-download endpoints (`GET /file`, `GET /files/`, `PUT /files/`) that convert a client-supplied URI directly to a filesystem path and stream the file, without confining it to the workspace or any allow-listed root. In browser (non-Electron) deployments the connection token is enforced only on WebSocket upgrades; the HTTP middleware in `@theia/core` re-issues the cookie and calls `next()` without rejecting tokenless HTTP requests, so these endpoints are reachable without a valid token. As a result an unauthenticated client can read any file readable by the backend process, including files outside the opened workspace (for example `/etc/hosts`, SSH keys, or tokens). Electron mode uses a separate `ElectronSecurityToken` and is not affected via this path.	2026-08-05	7.5	CVE-2026-61891
Efstratios Goudelis--Ground Station	Ground Station prior to 0.6.0 contains an unauthenticated database-destruction and arbitrary-data-injection vulnerability in the Socket.IO server's database_backup event handler that allows any unauthenticated network peer to wipe or replace the entire SQLite database by sending a single full_restore command with a caller-supplied SQL blob. Attackers can connect to the Socket.IO server on port 7000 without credentials due to disabled authentication enforcement and a wildcard CORS policy, then emit the database_backup event to drop every existing table and recreate the database from attacker-controlled CREATE TABLE and INSERT INTO statements executed via raw exec_driver_sql, permanently destroying all satellite records, orbital sources, hardware configurations, and observation schedules, or planting fabricated orbital-source URLs and observation entries that redirect the ground station to attacker-controlled servers on the next scheduled sync.	2026-08-06	9.1	CVE-2026-53984
Efstratios Goudelis--Ground Station	Ground Station prior to 0.6.0 contains an unauthenticated blind server-side request forgery vulnerability in the orbital-source configuration path that allows any unauthenticated Socket.IO client to cause the ground-station process to issue outbound HTTP requests to attacker-chosen destinations. Attackers can connect to the Socket.IO server on port 7000 without credentials due to disabled authentication enforcement and a wildcard CORS policy, then submit a data_submission event with submit-orbital-sources action to persist an attacker-supplied URL in the database, then trigger an orbital sync via the equally unauthenticated background_task:start event. The URL is stored with no scheme allowlist, no host validation, and no rejection of loopback, RFC1918, or link-local (cloud instance metadata at 169.254.169.254) addresses, and is passed directly to requests.get in _fetch_http_3le and _fetch_http_omm in backend/tlesync/source_adapters.py. HTTP status codes and error messages from the outbound request are emitted in the orbital_sync_state Socket.IO event to all	2026-08-06	8.6	CVE-2026-53983

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	connected clients, providing a serviceable oracle for interpreting internal-service and cloud-metadata responses even though the raw response body is not directly leaked. Because the malicious source persists in the database across restarts and re-fires every 24 hours on the scheduled sync cycle, the primitive gives durable long-term SSRF without the attacker needing to remain connected.			
Efstratios Goudelis--Ground Station	Ground Station prior to 0.6.0 contains an unauthenticated denial-of-service vulnerability in the Socket.IO server's service_control event handler that allows any unauthenticated network peer to forcibly terminate the ground-station process by sending a single restart_service command. Attackers can connect to the Socket.IO server on port 7000 without credentials due to disabled authentication enforcement and a wildcard CORS policy, then emit the service_control event to terminate all active satellite-tracking sessions, SDR recording pipelines, demodulators, decoders, and rotator controllers, with repeated triggering possible in Docker deployments to create a persistent denial-of-service condition.	2026-08-06	7.5	CVE-2026-53985
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.9, 40.9.2, 41.2.2, and 42.0.0-beta.5, apps that expose Promise-returning functions to web content via contextBridge may be vulnerable to a context isolation bypass. Untrusted web content could obtain access to the isolated preload world and, through it, every capability the preload script has. In renderers without a sandbox, or with nodeIntegration enabled, this may escalate to Node.js access. Apps are affected if they expose Promise-returning functions via contextBridge, the standard pattern for wrapping ipcRenderer.invoke, in windows that load untrusted content. This issue is fixed in versions 39.8.9, 40.9.2, 41.2.2, and 42.0.0-beta.5.	2026-08-05	7.5	CVE-2026-70601
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.10, 40.9.3, 41.4.0, and 42.0.0, a custom scheme registered with supportFetchAPI: true but without corsEnabled: true was not subject to CORS enforcement. A page loaded from a remote origin could therefore fetch() or XMLHttpRequest that scheme cross-origin and read the full response body, rather than the read being blocked. Apps that serve sensitive data from such a scheme and load remote or untrusted content in a renderer are affected. This issue is fixed in versions 39.8.10, 40.9.3, 41.4.0, and 42.0.0.	2026-08-05	7.4	CVE-2026-70604
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.10, 41.10.3, and 42.0.1, a sandboxed iframe without the allow-popups keyword could still open a new window or trigger setWindowOpenHandler with no user interaction because new-window navigations taking the OpenURL path did not apply the iframe sandbox popup restriction. Apps that embed untrusted content in sandboxed iframes and rely on the absence of allow-popups to prevent window creation are affected, while apps that deny window creation in setWindowOpenHandler or do not embed untrusted content in sandboxed iframes are not affected. This issue is fixed in 39.8.10, 41.10.3, and 42.0.1.	2026-08-05	7.2	CVE-2026-70608
emlog--emlog	Emlog Pro through 2.6.23 contains a disabled TLS certificate validation vulnerability in include/service/ai.php that allows network-adjacent attackers to intercept outbound HTTPS requests to configured LLM providers by presenting arbitrary TLS certificates, as CURLOPT_SSL_VERIFYPEER and CURLOPT_SSL_VERIFYHOST are unconditionally disabled across sendStream(), sendImageRequest(), send(), and fetchSearchHtml() with no option to re-enable verification. Attackers can perform man-in-the-middle interception to extract Authorization Bearer API keys from every AI request and inject crafted AI responses that may be acted upon by the tool-call execution pipeline, including the query_database and update_config tool handlers.	2026-08-03	7.4	CVE-2026-67598
ESAFENET--CDG	A vulnerability was identified in ESAFENET CDG up to 20260615. Affected is an unknown function of the file /CDGServer3/ukey/usbkey/logindojojs. Such manipulation of the argument keyid leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	7.3	CVE-2026-18859
esphome--esphome	ESPHome through 2026.7.0-dev contains an operator-precedence bug in the cv.url() validator in esphome/config_validation.py: `if parsed.scheme and parsed.netloc or parsed.scheme == "file": return parsed.geturl()`. Because `and` binds tighter than `or`, any file: URI passes validation regardless of netloc. This validator gates the `url:` field of the external_components YAML directive's git source schema, which is passed to `git clone` (git supports file:// natively). A crafted `external_components` block with `url: "file:///attacker/repo"` clones an	2026-08-05	8.6	CVE-2026-71259

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker-controlled local path, which is then added to Python's import machinery via ESPHome's component loader, executing arbitrary Python code when the YAML configuration is processed (e.g. via `esphome config`/`esphome run`).			
Eukaryot--sonic3air	Sonic 3 A.I.R. before commit 2492d18 contains an unbounded memory allocation vulnerability in ReceivedPacketCache::enqueuePacket() that allows unauthenticated remote attackers to crash the server process by sending a crafted UDP packet with mUniquePacketID set to the maximum uint32 value. The mUniquePacketID field is read directly from the UDP wire-format packet header without bounds checking, causing the server to allocate one Cacheltem per missing packet ID gap, exhausting available host memory and propagating an uncaught std::bad_alloc exception to std::terminate().	2026-08-06	7.5	CVE-2026-66733
Facebook--Facebook for WooCommerce	Unauthenticated Cross Site Scripting (XSS) in Facebook for WooCommerce <= 3.7.5 versions.	2026-08-06	7.1	CVE-2026-66707
Facebook--Facebook for WordPress	Unauthenticated Cross Site Scripting (XSS) in Facebook for WordPress <= 5.2.1 versions.	2026-08-06	7.1	CVE-2026-66705
facelessuser--pymdown-extensions	pymdown-extensions is a collection of extensions for the Python Markdown library. In versions up to and including 11.0, four inline processors (caret, tilde, betterem, and magiclink) use regular expressions whose content groups can partition a run of delimiter characters in exponentially many ways, causing catastrophic backtracking. As a result, a single untrusted Markdown line under 50 bytes rendered with markdown.markdown() in each extension's default configuration drives the rendering thread into unbounded CPU usage that grows exponentially with input length, enabling an unauthenticated remote attacker who can submit Markdown to cause denial of service. The exposure is concrete for web applications that render user-supplied Markdown (comments, wikis, issue bodies, live preview), including any app using pymdownx.extra which bundles the vulnerable betterem default, as well as hosted docs/CI systems that build untrusted Markdown. The issue has been fixed in version 11.0.1.	2026-08-06	7.5	CVE-2026-67422
FFmpeg--FFmpeg	FFmpeg versions from 0.5 up to, but not including, 9.0 contain a signed integer overflow vulnerability in the DVB subtitle parser in libavcodec/dvbsub_parser.c that allows attackers to trigger a heap buffer overflow by supplying a crafted WTV file. The overflow causes the bounds-check guard expression to wrap to INT_MIN, bypassing the PARSE_BUF_SIZE comparison and invoking memcpy() with attacker-controlled data into a heap buffer, resulting in an out-of-bounds heap write and potential memory corruption or code execution.	2026-08-06	7.8	CVE-2026-70628
FFmpeg--FFmpeg	FFmpeg versions from 4.4 up to, but not including, 9.0 contain an out-of-bounds heap write vulnerability in the native GoPro CineForm HD (CFHD) decoder that allows remote attackers to corrupt heap memory by supplying a crafted AVI file during stream probing. The cfhd_decode() function fails to enforce the non-Bayer logical output-width invariant in the transform-type-2 reconstruction path, causing horiz_filter_clip() to write oversized 16-bit sample rows far beyond the allocated output frame buffer, which can be escalated to arbitrary code execution via overwrite of a live cleanup callback pointer.	2026-08-06	7.8	CVE-2026-70632
Flarum--Flarum Framework	Flarum before 1.8.16 contains a password reset token expiry bypass vulnerability that allows unauthenticated attackers to reuse expired password reset tokens by submitting them directly to the reset processing endpoint. The SavePasswordController::handle() method calls PasswordToken::findOrFail() without performing any expiry validation, allowing attackers to bypass the 24-hour token lifetime enforced only during form rendering and change any account's password to gain an authenticated session.	2026-08-05	8.1	CVE-2026-39923
fledge-iot--fledge	Fledge's backup-restore upload handler, upload_backup() (python/fledge/services/core/api/backup_restore.py), takes the first extracted tar member's filename (tar_file_names[0]) and builds a shell command via string formatting: `cmd = "cp {} {}".format(source, backup_path); ret_code = os.system(cmd)`. The only pre-check on the filename is a prefix/suffix match (startswith(backup_prefix), endswith(valid_extensions)), which a name such as `fledge_backup_\${id>/tmp/pwn}.db` satisfies while still injecting a shell command substitution. Because os.system() invokes a shell and no quoting (shlex.quote, list-form subprocess) is applied, an admin uploading a crafted backup archive achieves arbitrary OS command execution.	2026-08-05	7.2	CVE-2026-71284
FlowiseAI--Flowise	Flowise through 3.1.4 contains an insecure direct object reference vulnerability in the OpenAI Assistants integration that allows authenticated attackers to access	2026-08-06	9.9	CVE-2026-67622

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	credentials belonging to other workspaces by supplying an arbitrary credential UUID to Assistants endpoints without workspace ownership verification. Attackers can enumerate cross-workspace assistant metadata, retrieve file and vector store listings, and upload files into victim workspaces by exploiting the missing workspace-scoped authorization check in the credential lookup logic.			
FlowiseAI--Flowise	Flowise through 3.1.4 contains a server-side request forgery vulnerability in the SSRF guard implemented in httpSecurity.ts, where the DEFAULT_DENY_LIST omits the Oracle Cloud Infrastructure metadata endpoint 192.0.0.192 and the Alibaba Cloud metadata endpoint 100.100.100.200, allowing authenticated attackers to force the server to issue arbitrary GET requests to cloud instance metadata services. Attackers can send requests to the fetch-links API endpoint with a crafted URL parameter, bypassing deny-list validation including redirect-based bypasses, to reach instance metadata services and expose instance identity data and role credentials on Oracle Cloud Infrastructure or Alibaba Cloud deployments, with unauthenticated access possible when URL-fetching nodes exist in public chatflows.	2026-08-08	7.7	CVE-2026-67620
FlowiseAI--Flowise	Flowise through 3.1.4 contains a missing authorization vulnerability that allows authenticated workspace members to perform unauthorized document store operations by accessing unprotected mutation endpoints. Attackers holding only view-level permissions can send direct HTTP requests to the upsert and refresh document store routes to trigger document ingestion, refresh vector database contents, consume embedding API credits, and modify knowledge bases used by downstream chatflows.	2026-08-06	7.6	CVE-2026-67621
FlowiseAI--Flowise	Flowise through 3.1.4 contains an authentication bypass vulnerability that allows unauthenticated attackers to access the OAuth2 credential refresh endpoint by exploiting prefix-based whitelist matching in the authentication middleware defined in packages/server/src/utis/constants.ts. Attackers can send a POST request to the oauth2-credential refresh route with a trailing credential identifier to bypass all authentication and authorization checks, triggering unauthorized OAuth token rotation against credentials belonging to any workspace and potentially disrupting dependent OAuth integrations. This is a bypass of CVE-2026-41273.	2026-08-06	7.5	CVE-2026-70636
Foxit Software Inc.--Foxit PDF Services API	The PDF creation feature of Foxit PDF Services API supports referencing external files. Although local file access is restricted, an attacker could trigger an SSRF vulnerability by using URL redirection to bypass validation, leading to information disclosure.	2026-08-06	8.5	CVE-2026-18597
frappe--frappe	Frappe is a full-stack web application framework. Versions 14.96.9 and below, and 15.0.0 through 15.71.0 have an insecure endpoint parameter that is vulnerable to error-based SQL Injection through lack of validation. Sensitive information such as versioning can be retrieved. This issue is fixed in versions 14.96.10 and 15.72.0.	2026-08-07	8.1	CVE-2025-58375
Gen Digital--CCleaner	Link following vulnerability in the Uninstaller component in CCleaner prior to 7.10.1464 on Windows allows a local, low-privileged attacker to escalate privileges to SYSTEM via a symlink/junction created during application uninstallation, which CCleaner follows when deleting the application's data folder with elevated integrity.	2026-08-05	7.8	CVE-2026-12410
GeoVision Inc.--GV-AS1620 (AS-Manager)	The product firmware contains an embedded, static RSA private key utilized by the Lighttpd web server for TLS termination. Exposure of this private key allows malicious actors to breach the confidentiality and integrity of HTTPS communications, enabling traffic decryption and server spoofing.	2026-08-04	9.1	CVE-2026-18753
GeoVision Inc.--GV-AS1620 (GV-Cloud)	The product firmware contains an embedded, static RSA private key utilized by the Lighttpd web server for TLS termination. Exposure of this private key allows malicious actors to breach the confidentiality and integrity of HTTPS communications, enabling traffic decryption and server spoofing.	2026-08-04	9.1	CVE-2026-18754
GeoVision Inc.--GV-ASManager	A DLL hijacking vulnerability in GeoVision GV-ASManager allows a local attacker with write access to an unsafe search directory to execute arbitrary code. By placing a crafted dynamic-link library (DLL) file into the application search path prior to the legitimate library, the malicious code is loaded and executed under the security privileges of the GV-ASManager process.	2026-08-04	7.3	CVE-2026-18755
getgrav--grav	Grav CMS versions 2.0.7 through 2.0.10 fail to validate fully-qualified static method calls (Class::method) in blueprint dynamic-field directives because Blueprint::isSafeDynamicCall() only applies its dangerous-callable denylist to strings that do not contain '::.'. An account with only page-editing rights (admin.pages, not super-admin or admin.pages_twig) can plant a directive in a page's form-field frontmatter that invokes an arbitrary public static PHP method with attacker-	2026-08-03	8.1	CVE-2026-69088

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	controlled arguments. Using built-in gadget methods this allows reading of any server-readable file (disclosed to anonymous visitors of the crafted page) and arbitrary creation/copying of files and directories under the web-server account. Fixed in 2.0.11.			
getgrav--grav	Grav CMS 2.0.10 contains a path traversal vulnerability in ImageMedium::watermark(), which passes its unsanitized \$image argument to RocketTheme\Toolbox\ResourceLocator\UniformResourceLocator::findResource(). Because the file:// scheme branch only lexically collapses '..' segments without a realpath/containment check, an editor authoring Markdown image syntax with traversal sequences can cause arbitrary image files outside Grav's media sandbox to be composited into a carrier image, which is then cached and served from a public, unauthenticated URL - disclosing those files to anonymous visitors.	2026-08-03	7.5	CVE-2026-69089
ggml-org--llama.cpp	llama.cpp builds b4882 through b9058 contain a heap buffer overflow vulnerability in the KV cache state restore path where the state_read_data() function computes write size without overflow checking, allowing attackers with write access to the slot_save_path directory to corrupt heap memory. Attackers can craft malicious state files where cell_count multiplication overflows or exceeds tensor buffer allocation to write attacker-controlled bytes past buffer boundaries, potentially resulting in heap metadata corruption, model weight corruption, or arbitrary code execution via function pointer overwrite.	2026-08-06	8.1	CVE-2026-43629
ggml-org--llama.cpp	llama.cpp builds b7492 through the latest b9060 contains a use-after-free vulnerability in the vocab pointer of llama-server when the --sleep-idle-seconds feature is enabled, allowing unauthenticated remote attackers to execute arbitrary code. Attackers can trigger the vulnerability by sending requests to affected endpoints while the server transitions to sleep mode, causing concurrent worker threads to dereference a freed vocab pointer that can be reclaimed with attacker-controlled data to achieve remote code execution.	2026-08-06	8.1	CVE-2026-43631
ggml-org--llama.cpp	llama.cpp builds b7492 through the latest b9060 contains a use-after-free vulnerability in llama-server affecting six tokenization endpoints (/tokenize, /detokenize, /infill, /apply-template, /rerank, and /anthropic/count_tokens) that bypass the task queue and access ctx_server.vocab directly on HTTP worker threads. Attackers can exploit a time-of-check-time-of-use race condition where the main thread destroys and frees vocab after the synchronization lock is released but before the handler finishes using it, causing a crash or potential code execution when --sleep-idle-seconds is configured.	2026-08-06	8.1	CVE-2026-43632
ggml-org--llama.cpp	llama.cpp builds b1886 through b7445 contain a double free vulnerability in the LLaMA-Android JNI wrapper where new_1batch() allocates memory using malloc() while free_1batch() deallocates it using the C++ delete operator, causing heap metadata corruption. Attackers can trigger this memory management mismatch to cause denial of service through process crashes or potentially achieve arbitrary code execution depending on allocator state.	2026-08-06	7.8	CVE-2026-43622
ggml-org--llama.cpp	llama.cpp builds b1283 through b9058 contain an integer overflow vulnerability in the llama_batch_init() function where unchecked multiplications in malloc() calls can wrap past INT32_MAX when computing allocation sizes. Attackers can pass specially crafted parameters to trigger integer overflow, causing heap corruption and potentially achieving arbitrary code execution through subsequent batch operations that write past allocated buffer boundaries.	2026-08-06	7.8	CVE-2026-43627
ggml-org--llama.cpp	llama.cpp builds b3978 through b9058 contain an integer underflow and out-of-bounds read vulnerability in the DRY sampler that allows unauthenticated attackers to trigger a heap buffer underflow by sending a crafted HTTP request with dry_allowed_length set to INT32_MIN to the /v1/completions or /v1/chat/completions endpoints. Attackers can exploit this vulnerability to crash the server with SIGSEGV causing denial of service for all connected users, or corrupt token sampling probabilities by reading garbage values from memory before the allocated buffer.	2026-08-06	7.8	CVE-2026-43628
ggml-org--llama.cpp	llama.cpp builds b1886 through b7445 contain an integer overflow vulnerability in the LLaMA-Android JNI wrapper where the new_1batch() function multiplies sizeof(llama_seq_id) by an attacker-controlled n_seq_max parameter without overflow validation, causing heap buffer allocation to wrap and allocate insufficient memory. Attackers can exploit this by providing a crafted n_seq_max value through a malicious model file or JNI call to trigger heap corruption and achieve denial of service or arbitrary code execution on Android applications using the LLaMA-Android binding.	2026-08-06	7.8	CVE-2026-70638

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ggml-org--llama.cpp	llama.cpp builds b1886 through b7445 contain a race condition use-after-free vulnerability in the LLaMA-Android JNI wrapper where bench_1model() and free_1context() lack synchronization, allowing Thread A to operate on freed memory while Thread B concurrently frees the llama_context. Attackers can exploit this by performing heap spray with attacker-controlled data containing a fake vtable to hijack the vtable pointer at offset +0x30, causing llama_batch_allocr::clear() to dereference arbitrary memory and achieve remote code execution.	2026-08-06	7	CVE-2026-70640
Gitea--Gitea	Gitea prior to 1.27.0 contains a server-side request forgery vulnerability that allows authenticated attackers to bypass SSRF protections by exploiting HTTP fetch operations in migration and OAuth avatar code paths that use Go's default http.Get without a custom DialContext. Attackers can supply arbitrary URLs through release asset download URLs, pull-request patch URLs, or OAuth avatar endpoints to reach internal services, cloud instance-metadata endpoints, or read local files such as the application configuration containing database credentials and signing secrets, with exfiltrated content persisted as migration release assets for later retrieval.	2026-08-05	7.6	CVE-2026-34966
gitpython-developers--GitPython	GitPython before 3.1.53 fails to properly escape section names in git config files, allowing attackers to inject arbitrary configuration directives through malicious submodule names. Attackers can inject core.sshCommand or other dangerous config keys into the victim's .git/config via create_submodule or clone_from operations, achieving remote code execution when git performs ssh operations.	2026-08-03	7	CVE-2026-69097
gitroomhq--postiz-app	Postiz is an open-source social media scheduling tool. The route that serves locally stored media joins URL-supplied path segments onto the upload directory and streams the file without normalising the path or confining it to that directory, and the route requires no authentication. Raw dot-segments are collapsed before routing, but URL-encoded separators survive route matching and are decoded only once they reach the handler, restoring the traversal at the filesystem call. An unauthenticated remote attacker can therefore read any file readable by the application process, including the process environment, which exposes the JWT signing secret, the database connection string, and connected provider and billing secrets. Because session tokens are signed with that secret and carry no expiry, this allows forging a non-expiring session as any user, including an administrator, without a password.	2026-08-07	9.8	CVE-2026-19264
GL-iNet--GL-MT3000	A flaw has been found in GL-iNet GL-MT3000 up to 4.4.5. This vulnerability affects the function plugins.remove_package/plugins.install_package of the file /cgi-bin/glc of the component plugins.so Native Plugin. This manipulation causes command injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	9.8	CVE-2026-18612
GL-iNet--GL-MT3000	A vulnerability has been found in GL-iNet GL-MT3000 up to 4.4.5. This issue affects the function plugins.set_config of the file /cgi-bin/glc of the component plugins.so Native Plugin. Such manipulation leads to injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	9.8	CVE-2026-18613
GL-iNet--GL-MT3000	A vulnerability was found in GL-iNet GL-MT3000 up to 4.4.5. Impacted is the function s2s.enable_echo_server of the file /cgi-bin/glc of the component s2s.so Native Plugin. Performing a manipulation of the argument port results in command injection. The attack may be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	9.8	CVE-2026-18614
GL-iNet--GL-MT3000	A vulnerability was determined in GL-iNet GL-MT3000 up to 4.4.5. The affected element is the function wg-server.generate_publickey of the file /cgi-bin/glc of the component wg-server.so Native Plugin. Executing a manipulation of the argument private_key can lead to command injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	9.8	CVE-2026-18615
GL-iNet--GL-MT3000	A vulnerability was identified in GL-iNet GL-MT3000 up to 4.4.5. The impacted element is the function server.set_peer of the file /cgi-bin/glc of the component wg-server.so Native Plugin. The manipulation of the argument public_key leads to command injection. Remote exploitation of the attack is possible. The exploit is	2026-08-03	9.8	CVE-2026-18616

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	publicly available and might be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.			
GL.iNet--AX1800	A vulnerability was identified in GL.iNet AX1800 up to 4.8.3. The affected element is the function <code>remove_rule</code> of the file <code>/usr/share/gl-ngx/oui-rpc.lua</code> of the component RPC Endpoint. The manipulation of the argument <code>args.id</code> leads to command injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	2026-08-04	8.8	CVE-2026-18787
GL.iNet--GL-MT3000	A vulnerability was found in GL.iNet GL-MT3000 up to 4.4.5. This impacts the function <code>ovpn-client.check_config</code> of the file <code>/cgi-bin/glc</code> of the component <code>ovpn-client.so</code> Native Plugin. Performing a manipulation of the argument <code>filename</code> results in command injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	9.8	CVE-2026-18601
GL.iNet--GL-MT3000	A vulnerability was determined in GL.iNet GL-MT3000 up to 4.4.5. Affected is the function <code>ovpn-client.get_recommend_config</code> of the file <code>/cgi-bin/glc</code> of the component <code>ovpn-client.so</code> Native Plugin. Executing a manipulation of the argument <code>Hostname</code> can lead to command injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	9.8	CVE-2026-18602
GL.iNet--GL-MT3000	A weakness has been identified in GL.iNet GL-MT3000 up to 4.4.5. This issue affects the function <code>remove_profile</code> of the file <code>/cgi-bin/glc</code> of the component <code>modem.so</code> . This manipulation causes command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	9.8	CVE-2026-18684
GL.iNet--GL-MT3000	A security vulnerability has been detected in GL.iNet GL-MT3000 up to 4.4.5. Impacted is the function <code>set_upgrade</code> of the file <code>/cgi-bin/glc</code> of the component <code>modem.so</code> . Such manipulation leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	9.8	CVE-2026-18685
GL.iNet--GL-MT3000	A vulnerability was detected in GL.iNet GL-MT3000 up to 4.4.5. The affected element is the function <code>nas-web.add_user</code> of the file <code>/cgi-bin/glc</code> of the component <code>nas-web</code> RPC Wrapper. Performing a manipulation results in command injection. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-04	9.8	CVE-2026-18686
GL.iNet--GL-MT3000	A vulnerability was detected in GL.iNet GL-MT3000 up to 4.4.5. The affected element is the function <code>logread.get_system_log</code> of the file <code>/usr/lib/oui-httpd/rpc/logread</code> of the component Logread Lua RPC plugin. The manipulation of the argument <code>module</code> results in command injection. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	8.8	CVE-2026-18598
GL.iNet--GL-MT3000	A flaw has been found in GL.iNet GL-MT3000 up to 4.4.5. The impacted element is the function <code>logread.set_config</code> of the file <code>/usr/lib/oui-httpd/rpc/logread</code> of the component Logread Lua RPC Plugin. This manipulation of the argument <code>record_size</code> causes command injection. The exploit has been published and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	8	CVE-2026-18599
GL.iNet--GL-MT3000	A vulnerability has been found in GL.iNet GL-MT3000 up to 4.4.5. This affects the function <code>network.switch_info/network.switch_status</code> of the file <code>/usr/lib/oui-httpd/rpc/network</code> of the component Network Lua RPC Plugin. Such manipulation of the argument <code>switch</code> leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	8.8	CVE-2026-18600
go-git--go-git	go-git is an extensible git implementation library written in pure Go. Prior to 5.19.2 and 6.0.0-alpha.5, <code>worktree</code> operations (including <code>checkout</code> , <code>status</code> , and <code>add</code>) resolve symbolic links inside the working tree without confining resolution to the <code>worktree</code> boundary, so a maliciously crafted repository containing a symlink can cause go-git to read from or write to files outside the intended working directory	2026-08-07	7.1	CVE-2026-71556

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	when the repository is cloned and its worktree operations are used. Versions 5.19.2 and 6.0.0-alpha.5.			
go-shiori--shiori	Shiori's CheckToken function (internal/domains/auth.go) validates only the JWT's HMAC signature and returns the embedded claims.Account object unmodified, never re-fetching the account from the database. No session store or token-revocation mechanism exists in the codebase. Deleting an account or demoting it from owner to a regular role has no effect on tokens already issued to that account - a deleted or demoted owner's token continues authenticating with its original owner-level privileges until natural expiry, which can be up to 30 days with 'remember me' enabled.	2026-08-05	8.2	CVE-2026-71206
go-shiori--shiori	go-shiori's DownloadBookmark() (internal/core/download.go) fetches a caller-supplied bookmark URL using a plain http.Client with no custom DialContext or destination-IP validation (no IsLoopback(), IsPrivate(), IsUnspecified(), or IsLinkLocalUnicast() checks). An authenticated user creating or updating a bookmark via POST /api/bookmark, PUT /api/v1/bookmarks/cache, or POST /api/bookmarks/ext can supply a loopback (127.0.0.1) or 0.0.0.0 (which Linux redirects to loopback) URL, causing the server to make outbound requests to internal-only services, cloud metadata endpoints, or other network-restricted resources.	2026-08-05	8.5	CVE-2026-71280
google-maps-easy-pro--google-maps-easy-pro	Multiple Supsysic Pro plugins were distributed with malicious code through the vendor's compromised update server, allowing unauthenticated attackers to deploy a second-stage payload that exfiltrates credentials and other sensitive data and grants full control of affected sites.	2026-08-06	9.8	CVE-2026-17032
gopacket--gopacket	gopacket provides packet processing capabilities for Go. Through version 1.7.0, multiple layer decoders use attacker-controlled lengths, counts, or offsets before validating them against packet buffers, allowing a crafted packet decoded through DecodingLayerParser or DecodeFromBytes to trigger an unrecovered panic and remotely deny service. A patch commit is available at 210f25f.	2026-08-07	7.5	CVE-2026-65819
grocy--grocy	Grocy's API request-body parser (controllers/Api/BaseApiController.php, GetParsedAndFilteredRequestBody) purifies incoming field values with HTMLPurifier, then manually reverses HTML-entity encoding of the resulting output by replacing <, >, and & back to <, >, and & immediately after purification. This double-decode reconstructs live HTML/script tags from the entity-encoded form that HTMLPurifier produced to neutralize them, re-introducing stored XSS across API-writable fields (products, recipes, stock, users, chores, and others) that are rendered elsewhere without re-sanitization.	2026-08-05	8.7	CVE-2026-71236
guzzle--guzzle	Guzzle is an extensible PHP HTTP client. Prior to 7.15.2 and 8.0.1, Guzzle gives a transport the request URI as text and supplies the Host header separately. The cURL handlers set CURLOPT_URL to the URI exactly as written and push that Host into CURLOPT_HTTPHEADER; StreamHandler does the same through fopen(). libcurl then parses the authority itself, percent-decoding it and, on an IDN-capable build, applying IDNA mapping, and uses the result to resolve, connect, name the TLS peer and address a proxy CONNECT, while the supplied Host suppresses the aligned one libcurl would have generated. For a URI host written as 127.0.0.%31, filter_var() rejects the host as an IP literal, yet libcurl decodes it to 127.0.0.1 and reaches loopback with no DNS lookup while the server receives Host: 127.0.0.%31. An attacker who influences a fetched URI can therefore reach a host the application's checks excluded and read whatever the host exposes of the response. The same divergence moves Guzzle's own decisions onto a spelling the transport does not use: no_proxy selects proxy routing from the literal host, and RedirectMiddleware decides from it whether to strip Authorization and Cookie. Exploitation requires the application to build a request URI from untrusted input and to make a host decision before handing it to Guzzle. This issue is fixed in versions 7.15.2 and 8.0.1.	2026-08-03	7.2	CVE-2026-69246
H3C--NX15	A security vulnerability has been detected in H3C NX15 V100R017. Impacted is an unknown function of the file /api/wizard/networkSetup. Such manipulation leads to missing authentication. The attack may be performed from remote. The vendor was contacted early about this disclosure.	2026-08-04	7.3	CVE-2026-18810
H3C--NX15	A vulnerability was detected in H3C NX15 V100R017. The affected element is the function Add of the file /api/esps. Performing a manipulation of the argument esps.filter.url results in command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure.	2026-08-04	7.2	CVE-2026-18811

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
H3C--NX15	A flaw has been found in H3C NX15 V100R017. The impacted element is the function <code>esps.ipv6.wan</code> of the file <code>/api/esps</code> . Executing a manipulation of the argument <code>workMode</code> can lead to command injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure.	2026-08-04	7.2	CVE-2026-18812
H3C--NX15	A vulnerability has been found in H3C NX15 V100R017. This affects the function <code>delete</code> of the file <code>/api/esps</code> . The manipulation of the argument <code>esps.apcm.version</code> leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.	2026-08-04	7.2	CVE-2026-18813
H3C--NX15	A vulnerability was found in H3C NX15 V100R017. This impacts the function <code>reload.reload_config</code> of the file <code>/api/esps</code> . The manipulation results in command injection. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure.	2026-08-04	7.2	CVE-2026-18814
H3C--NX15	A weakness has been identified in H3C NX15 V100R017. This impacts the function <code>file.exec</code> of the file <code>/api/esps</code> of the component Backend RPC. This manipulation of the argument <code>File</code> causes <code>os</code> command injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure.	2026-08-05	7.2	CVE-2026-18900
H3C--NX15	A security vulnerability has been detected in H3C NX15 V100R017. Affected is the function <code>service.add</code> of the file <code>/api/esps</code> of the component Web API. Such manipulation leads to exposed dangerous routine. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure.	2026-08-05	7.2	CVE-2026-18901
H3C--NX15	A vulnerability was detected in H3C NX15 V100R017. Affected by this vulnerability is the function <code>esps.wan.repeater.set/repeaterproc</code> of the file <code>/api/esps</code> . Performing a manipulation of the argument <code>my2P4key</code> results in command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure.	2026-08-05	7.2	CVE-2026-18902
Hamid Alinia-- Login with phone number	Unauthenticated Bypass Vulnerability in Login with phone number <= 1.8.70 versions.	2026-08-06	8.1	CVE-2026-65570
hapifhir-- org.hl7.fhir.core	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.11, the JSON utility parser in <code>org.hl7.fhir.utilities.json.parser.JsonParser</code> enforces no maximum nesting depth for arrays or objects. As a result, a small but deeply nested, syntactically valid FHIR JSON document can trigger unbounded <code>readArray()</code> or <code>readObject()</code> recursion, raising a <code>StackOverflowError</code> before structural validation runs. An attacker who can submit JSON resources for validation can thus crash the request thread, and services that do not isolate <code>StackOverflowError</code> safely may experience worker loss or process instability - a denial-of-service condition. This issue is fixed in version 6.9.11.	2026-08-07	7.5	CVE-2026-62295
hapifhir-- org.hl7.fhir.core	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.11, <code>XhtmlParser.java</code> imposes no maximum element nesting depth, so a deeply nested <code>text.div</code> narrative triggers unbounded recursion between <code>parseElementInner()</code> and <code>parseElement()</code> , raising a <code>StackOverflowError</code> . An attacker who can submit FHIR resources containing such narratives can thus crash a parsing or validation worker thread, affecting validator services and any application that parses attacker-supplied FHIR JSON or XML. This issue is fixed in version 6.9.11.	2026-08-07	7.5	CVE-2026-62296
Harsh21Patel-- Inventory- Management- System-PHP	Inventory-Management-System-PHP's <code>login.php</code> constructs its authentication query via direct string concatenation of raw POST parameters: <code>\$sql = "select * from user where email = '\$email' and password = '\$password'"</code> , with no escaping or parameterization, allowing authentication bypass via a payload such as <code>email=' OR 1=1 LIMIT 1-- --</code> . Separately, <code>delete.php</code> executes <code>mysqli_query(\$db, "DELETE FROM product WHERE product_id=" . \$_GET['id'])</code> with no authentication check and no validation of the <code>id</code> parameter, allowing an unauthenticated attacker to delete arbitrary product rows or perform blind SQL injection via payloads such as <code>id=0 OR SLEEP(5)</code> .	2026-08-05	9.8	CVE-2026-71248
HashBrownCMS-- hashbrown-cms	HashBrown CMS through 1.4.6 contains an OS Command Injection vulnerability (CWE-78) in the media upload thumbnail generation routine. <code>Media.generateThumbnail()</code> in <code>src/Server/Entity/Resource/Media.js</code> builds a temporary file path as <code>'thumbnail' + Path.extname(filename)</code> and passes it, unescaped, into a shell command executed via <code>AppService.exec()</code> (<code>'convert ' +</code>	2026-08-05	8.8	CVE-2026-70374

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	tempFile + ...). The MIME-type filter in getMimeType() (src/Common/utilities.js) truncates the extracted extension at the first '?' character, while Path.extname() does not, allowing a filename such as 'x.jpg?\$(command)' to pass the image-type check while still injecting a shell command substitution into the exec() call. An authenticated user holding the media resource scope can achieve arbitrary OS command execution in the context of the Node.js process via POST /api/{project}/{environment}/media/new.			
HashBrownCMS--hashbrown-cms	HashBrown CMS through 1.4.6 contains an OS Command Injection vulnerability (CWE-78) in the Git deployer component. GitDeployer.pullRepo() in src/Server/Entity/Deployer/GitDeployer.js executes AppService.exec('git checkout \${this.branch} 'master)'), interpolating the configured branch value directly into a shell command with no escaping. GitDeployer.validate() only rejects a single-quote character in the repo, branch, username, and password fields; shell metacharacters such as ';', '&&', ' ', backticks, and '\$()' are not filtered. A user able to configure a project's Git deployer settings can set a malicious branch value (e.g. 'master;<command>#') that executes automatically on every subsequent deployer operation (media upload, content save, etc.), since pullRepo() is invoked unconditionally at the start of each such operation. This is related to CVE-2020-6948, which addressed single-quote escaping of the repo, username, and password fields in the same file's git clone invocation; the branch field used in the unquoted git checkout command was not covered by that fix and remains injectable.	2026-08-05	8.8	CVE-2026-70375
HashiCorp--Consul	Consul Community Edition and Consul Enterprise 1.13.0 through 2.0.2 are vulnerable to an unauthenticated denial of service through unbounded connection acceptance on the external gRPC listeners. A remote attacker may exhaust agent file descriptors, goroutines, and memory by opening many incomplete connections, potentially preventing legitimate clients from connecting. This vulnerability, CVE-2026-15972, is fixed in Consul 2.0.3 and Consul Enterprise 1.21.17, 1.22.11, and 2.0.3.	2026-08-07	7.5	CVE-2026-15972
HAVELSAN Inc.--Liman MYS	Missing Authorization vulnerability in HAVELSAN Inc. Liman MYS allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Liman MYS: from 2.2.3 before 2.3.1.	2026-08-04	8.8	CVE-2026-17070
HAVELSAN Inc.--Liman MYS	Missing Authorization vulnerability in HAVELSAN Inc. Liman MYS allows Privilege Escalation. This issue affects Liman MYS: from 2.2.3 before 2.3.1.	2026-08-04	8.8	CVE-2026-18650
heshengtao--super-agent-party	A vulnerability has been found in heshengtao super-agent-party up to 0.4.1. The impacted element is the function sanitize_proxy_url of the file server.py of the component extension_proxy Route. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	7.3	CVE-2026-18973
Hewlett Packard Enterprise (HPE)--EdgeConnect SD-WAN Orchestrator	Multiple vulnerabilities in the REST API interface of HPE Networking SD-WAN Orchestrator could allow an unauthenticated remote attacker to bypass web authentication mechanisms and access system functions. Successful exploitation could allow an attacker to view and modify potentially sensitive information on the target system.	2026-08-04	9.8	CVE-2026-63455
Hewlett Packard Enterprise (HPE)--EdgeConnect SD-WAN Orchestrator	Multiple vulnerabilities in the REST API interface of HPE Networking SD-WAN Orchestrator could allow an unauthenticated remote attacker to bypass web authentication mechanisms and access system functions. Successful exploitation could allow an attacker to view and modify potentially sensitive information on the target system.	2026-08-04	9.8	CVE-2026-63456
HKUDS--LightRAG	LightRAG provides simple and fast retrieval-augmented generation. Through version 1.5.4, the LightRAG API server binds to all network interfaces with authentication disabled by default, allowing an unauthenticated network attacker to read indexed document content, upload or delete documents, modify the knowledge graph, cancel pipelines, clear caches, and consume LLM resources. This issue is mitigated in version 1.5.5rc1.	2026-08-07	9.8	CVE-2026-61808
ho3einie--Material Dashboard	The Material Dashboard plugin for WordPress is vulnerable to unauthorized access and modification of data due to missing capability checks on the amd_ajax_target_task_manager() function in all versions up to, and including, 1.4.10. This makes it possible for unauthenticated attackers to enumerate all scheduled tasks (potentially exposing PII), execute arbitrary tasks, and delete any task via the public_amd_ajax_handler AJAX action.	2026-08-05	7.3	CVE-2026-6079
home-assistant--core	Home Assistant is open source home automation software focused on local control and privacy. Prior to 2026.5.3, the Companion app treats tag links (NFC or QR) delivered through an OS-level routing mechanism as if they were physically	2026-08-07	7.1	CVE-2026-66060

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	scanned, without validating the calling app or prompting the user. As a result, any untrusted app on the device can forward an arbitrary tag to Home Assistant, causing it to execute the associated automation as though a legitimate user had scanned an authorized tag. This allows silent, unattended automation execution by untrusted local callers. This issue is fixed in version 2026.8.1.			
home-assistant--core	Home Assistant is open source home automation software focused on local control and privacy. Prior to 2026.5.0, the iOS Companion app treats tag links (NFC or QR) delivered through an OS-level routing mechanism such as iOS universal links as if they were physically scanned, without validating the calling app or prompting the user. As a result, any untrusted app on the device can forward an arbitrary tag to Home Assistant, causing it to execute the associated automation as though a legitimate user had scanned an authorized tag. This allows silent, unattended automation execution by untrusted local callers. This issue has been fixed in version 2026.5.0.	2026-08-07	7.1	CVE-2026-66061
huggingface--peft	Hugging Face peft's LoRA-GA and CorDA initialization modules (src/peft/tuners/lora/corda.py lines ~102 and ~163, and src/peft/tuners/lora/loraga.py line ~101) call torch.load() on config-specified cache/covariance files without weights_only=True, bypassing peft's own safe-loading wrapper used elsewhere in the codebase. Because torch.load() without weights_only=True performs full pickle deserialization, loading a malicious cache or covariance file (e.g. a shared/downloaded LoRA-GA or CorDA cache) results in arbitrary code execution.	2026-08-05	8.8	CVE-2026-71281
IBM--Application Gateway Operator	IBM Application Gateway Operator 22.2 through 26.06 is vulnerable to Server-Side Request Forgery (SSRF) due to insufficient validation of URLs specified in custom resources.	2026-08-05	8.5	CVE-2026-17617
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 could allow a remote authenticated attacker to execute arbitrary commands due to improper validation of the command field in MCP server configurations.	2026-08-05	8.8	CVE-2026-17623
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, and 1.0.0 through 1.10.3 could allow a remote authenticated attacker to execute arbitrary code due to improper validation of module imports.	2026-08-05	8.5	CVE-2026-17624
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 Langflow could allow an authenticated attacker to read, modify, or expose sensitive host files via Docker-based MCP servers due to incomplete filtering of dangerous Docker volume-mount and device-mapping arguments.	2026-08-05	8.8	CVE-2026-17626
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 could allow a remote authenticated attacker to execute arbitrary code due to improper validation of Python code during AST-based security scanning.	2026-08-05	8.8	CVE-2026-17632
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 could allow a remote authenticated attacker to execute arbitrary code due to code injection.	2026-08-05	8.5	CVE-2026-17633
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 installations allow anyone on the internet to execute arbitrary code on the server without any credentials via 2 HTTP requests.	2026-08-05	8.8	CVE-2026-8182
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 could allow a remote attacker to inject arbitrary code on the system, due to the improper control of user input code.	2026-08-05	8.8	CVE-2026-8478
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 Langflow allows remote authenticated attackers to bypass localhost-only restrictions and write arbitrary MCP server configurations to IDE configuration files on the host system.	2026-08-05	8.5	CVE-2026-9077
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 could allow an authenticated attacker to execute unintended code during Agentic Assistant validation due to improper handling of LLM-generated components. The application executes model-generated Python code in the backend during validation prior to user approval, which may allow an attacker to trigger side effects such as outbound network access, file system interaction, or data exfiltration with the privileges of the Langflow backend process.	2026-08-05	8.1	CVE-2026-9196
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 could allow an authenticated attacker to execute arbitrary code due to a cryptographic weakness in the custom component validation mechanism. When the optional hardening mode that restricts execution to trusted component templates is enabled, the application validates component code using a truncated SHA-256 hash. Because the hash comparison relies on only a portion of the digest, an attacker can craft malicious component code that collides with a trusted template hash and bypasses validation. Successful exploitation allows the attacker to introduce and execute unauthorized Python	2026-08-05	8.8	CVE-2026-9201

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	code within the Langflow process, defeating the intended security control and potentially leading to full compromise of the affected instance.			
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, and 1.0.0 through 1.10.3 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-05	7.2	CVE-2026-17625
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 could allow a remote attacker to execute arbitrary code due to improper validation of configuration parameters.	2026-08-05	7.2	CVE-2026-17630
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, and 1.0.0 through 1.10.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot " sequences (/.. /) to view arbitrary files on the system.	2026-08-05	7.7	CVE-2026-8183
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 contain an authentication bypass vulnerability in the Model Context Protocol (MCP) composer endpoint when mcp_composer_enabled=true (default) and projects are configured with auth_type=oauth .	2026-08-05	7.5	CVE-2026-8446
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, 1.0.0 through 1.10.3, and 1.0.0 through 1.10.3 use Python's non-cryptographic random module for generating Fernet encryption keys from user secrets under 32 characters. The deterministic Mersenne Twister PRNG produces identical keys for identical seeds, allowing attackers to reproduce encryption keys and decrypt stored API keys and authentication tokens.	2026-08-05	7.4	CVE-2026-8470
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3, and 1.0.0 through 1.10.3 contains a Server-Side Request Forgery (SSRF) vulnerability in the validate_model_provider_key() function for the Ollama provider. The function accepts a user-supplied OLLAMA_BASE_URL parameter and passes it directly to requests.get() without validation, scheme/host allowlisting, or filtering of private IP ranges (loopback, RFC1918, link-local addresses).	2026-08-05	7.1	CVE-2026-9081
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 contain an authorization bypass vulnerability in the MemoryComponent that allows authenticated users to access chat history of other users via session_id collision. The MemoryComponent.retrieve_messages and store_message methods filter on session_id without validating flow_id or user_id ownership, enabling cross-user information disclosure through multiple authenticated API endpoints including /api/v1/run/*, /api/v1/responses, and /api/v2/workflow/*. This vulnerability only affects multi-user deployments with LANGFLOW_AUTO_LOGIN=False.	2026-08-05	7.1	CVE-2026-9130
IBM--Langflow OSS	IBM Langflow OSS contains a weak cryptographic key derivation vulnerability in the ensure_fernet_key() function.	2026-08-05	7.4	CVE-2026-9205
IBM--QRadar	IBM QRadar 7.6.0.0 through 7.6.0.1, and 7.5.0 through 7.5.0 UP 15 Interim Fix 005 has an XML External Entity (XXE) injection vulnerability. The vulnerability resides in the parseXmlPayload() function within the event processing pipeline (q1labs_core.jar). When at least one log source type is configured to use XML-format property autodetection, the system processes XML-formatted syslog events sent to port 514 (UDP/TCP) without authentication.	2026-08-05	8.2	CVE-2026-10025
IBM--WebSphere Application Server	IBM WebSphere Application Server 8.5, and 9.0 and IBM WebSphere Application Server - Liberty Continuous delivery has a flaw in the ORB component in IBM SDK, Java Technology Edition, may allow a malicious IOP server to induce loading and instantiation of arbitrary classes.	2026-08-05	8.1	CVE-2026-8400
imranrisal-dev--Student-Management-System	A vulnerability was detected in imranrisal-dev Student-Management-System 18ea7904c339e0c7b0234724a79c939ce6191def/a8d43a29aaf267e7ca97171d6dbb44057bcd7f8c. Affected by this vulnerability is an unknown functionality of the file loginCheckTest.php of the component Login. The manipulation of the argument username/password results in sql injection. The attack can be launched remotely. The exploit is now public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	7.3	CVE-2026-18958
inisev--Backup Migration	The Backup Migration plugin for WordPress is vulnerable to OS Command Injection in all versions up to, and including, 2.1.5.1 due to insufficient sanitization of the 'file' POST parameter on the 'restoreBackup()' AJAX handler. The handler applies 'esc_attr()' - an HTML-context sanitizer that does not strip shell metacharacters - and concatenates the result, unquoted, into a 'php-cli -f-Â' bmi_restore <file> <remote>' command passed to 'exec()'. This makes it possible for authenticated	2026-08-05	7.2	CVE-2026-7693

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers, with Administrator-level access (or any user granted the plugin's `do_backups` capability) and above, to execute arbitrary OS commands as the web-server user, bypassing WordPress hardening constants such as `DISALLOW_FILE_EDIT` and `DISALLOW_FILE_MODS` that would otherwise prevent code execution from the admin UI. This is an incomplete fix of CVE-2023-7002, which patched the same pattern only in the `\$_POST['url']` path of `handleQuickMigration();` the equivalent mitigations (`rawurlencode()` + explicit shell-metachar replacement + double-quoting in `exec()`) were never applied to `\$backupName`.			
INQUIRELAB--mcp-bridge-api	A vulnerability was found in INQUIRELAB mcp-bridge-api up to b30a82aa1d1d1139e0de846c41c8aadee6e06114. The impacted element is an unknown function of the file mcp-bridge.js of the component Servers Endpoint. Performing a manipulation of the argument command/args results in command injection. It is possible to initiate the attack remotely. This product is using a rolling release to provide continuous delivery. Therefore, no version details for affected nor updated releases are available. The pull request to fix this issue awaits acceptance.	2026-08-08	7.3	CVE-2026-19263
Integrate PhonePe with WooCommerce--Integrate PhonePe with WooCommerce	The Integrate PhonePe with WooCommerce WordPress plugin through 1.2.1 does not validate that a verified payment transaction belongs to the order being marked as paid, nor does it verify the authenticity of its payment-completion request, allowing unauthenticated attackers to reuse a single valid transaction to mark arbitrary orders as paid and bypass payment.	2026-08-06	7.5	CVE-2026-10599
intelliants--subrion	Subrion CMS's admin grid sorting helper, `_gridGetSorting()` in includes/classes/ia.base.controller.admin.php, whitelists the `dir` (ASC/DESC) request parameter via in_array(), but falls back to the raw, attacker-supplied `sort` GET parameter whenever the requested key is not present in the per-controller `\$ _gridSorting` whitelist array: `\$column = isset(\$this->_gridSorting[\$params['sort']]) ? ... : \$params['sort'];`, which is then placed into `sprintf(' ORDER BY %s`%s` %s', \$tableAlias, \$column, \$direction)` with only backtick-quoting and no escaping. Because a backtick in the payload breaks out of the identifier context, an authenticated admin session can inject arbitrary SQL (error-based via EXTRACTVALUE, or time-based via SLEEP()) to extract database contents including administrator password hashes. Most of Subrion's ~29 admin grid controllers either define no `\$ _gridSorting` whitelist at all (e.g. pages.php, transactions.php, languages.php) or an incomplete one covering only some of their sortable columns (e.g. members.php whitelists only 1 of 7 sortable fields), making the vast majority of admin grid endpoints exploitable.	2026-08-05	7.2	CVE-2026-71292
invoiceninja--invoiceninja	InvoiceNinja v5-stable renders an invoice or quote's "terms" field in the client portal using Laravel Blade's raw output directive {!! \$entity->terms !!} (resources/views/portal/ninja2020/invoices/includes/terms.blade.php) with no HTML sanitization. StoreInvoiceRequest.php only strips newlines from the field and does not purify HTML. An authenticated user with invoice creation access can set the terms field via the REST API (PUT /api/v1/invoices/{id}) to an HTML/JavaScript payload that executes in the client's browser when they view the invoice, enabling session cookie theft and client account takeover. This is a distinct code path from the previously published invoice line-item description field XSS (GHSA-98wm-cxpw-847p / CVE-2026-33628).	2026-08-05	8.7	CVE-2026-71233
iot-ecology--rust-iot-platform	rust-iot-platform's AuthToken request-guard implementation (api/src/main.rs) only checks whether the Authorization HTTP header is present, and never validates its value against any session, token store, or signature. Any request carrying an arbitrary non-empty Authorization header (e.g. `Authorization: fake`) satisfies the guard, granting access to every endpoint protected only by this request guard.	2026-08-05	9.1	CVE-2026-71277
iot-ecology--rust-iot-platform	rust-iot-platform allows creating a "calc rule" via POST /calc-rule/create (api/src/controller/calc_rule_router.rs) containing an arbitrary `script` field. This route does not take the AuthToken request guard used elsewhere in the application, making it reachable without authentication. The stored script is subsequently executed via quick_js::Context::eval() in api/src/biz/calc_run_biz.rs with no sandboxing, allowing an unauthenticated attacker to achieve arbitrary JavaScript execution in the server process by creating and triggering a malicious calc rule.	2026-08-05	9.8	CVE-2026-71278
IoTSharp--IoTSharp	IoTSharp BlobStorageController.cs lacks the [Authorize] attribute applied to every other controller in the application (DevicesController, CustomersController, TenantsController, etc.), and no global authorization FallbackPolicy is configured in	2026-08-05	9.8	CVE-2026-71262

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Startup.cs, leaving its Upload/Download/List/Modify/Delete endpoints reachable by unauthenticated remote attackers. The path/filename parameters passed to these endpoints (e.g. `_blob.WriteFileAsync(\$"{path}/{formFile.FileName}", ...)`) are used without sanitization, enabling path traversal that allows writing, reading, modifying, and deleting arbitrary files outside the intended blob storage directory, including web-accessible paths that can be leveraged for remote code execution via webshell upload.			
ivanbebek--BOX NOW Delivery Croatia	Unauthenticated Broken Access Control in BOX NOW Delivery Croatia <= 3.3.0 versions.	2026-08-06	7.5	CVE-2026-65504
JeecgBoot--JeecgBoot	A vulnerability was identified in JeecgBoot up to 3.9.2. The affected element is an unknown function of the file /airag/chat/send of the component Anonymous Chat Attachment Parser. The manipulation leads to server-side request forgery. The attack can be initiated remotely. The exploit is publicly available and might be used. A fix is planned for the upcoming release.	2026-08-06	7.3	CVE-2026-19000
jegtheme--Jeg Kit for Elementor	Author PHP Object Injection in Jeg Kit for Elementor <= 3.2.10 versions.	2026-08-06	7.2	CVE-2026-65549
jetmonsters--JetFormBuilder	Unauthenticated Broken Access Control in JetFormBuilder <= 3.6.4.1 versions.	2026-08-06	7.5	CVE-2026-28140
Jiangmin--Antivirus	A flaw has been found in Jiangmin Antivirus 21. Impacted is the function MessageNotifyCallback in the library kvcore.sys of the component Minifilter Port. Executing a manipulation can lead to improper access controls. The attack needs to be launched locally. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-07	7.8	CVE-2026-19193
jina-ai--reader	A security vulnerability has been detected in jina-ai reader up to 1574bfd380d249c86c82db4dace0d9c8fe17e2b1. This issue affects the function isValidTLD of the file /backend/functions/src/cloud-functions/crawler.ts of the component Crawler/Puppeteer. The manipulation leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	7.3	CVE-2026-18647
Jordy Meow--AI Engine	Unauthenticated Cross Site Scripting (XSS) in AI Engine <= 3.6.8 versions.	2026-08-06	7.1	CVE-2026-65545
jp-secure--SiteGuard WP Plugin	Unauthenticated Cross Site Scripting (XSS) in SiteGuard WP Plugin <= 1.8.6 versions.	2026-08-06	7.1	CVE-2026-61982
juliangruber--brace-expansion	The brace-expansion library generates arbitrary strings containing a common prefix and suffix. Prior to 1.1.18, 2.1.4, 3.0.6, and 5.0.9, expand() does not apply maxLength while constructing comma-alternative intermediate arrays or padded sequences, allowing attacker-controlled input to exhaust memory or block the event loop. The fix for CVE-2026-14257 is bypassed by the vulnerability. This issue is fixed in versions 1.1.18, 2.1.4, 3.0.6, and 5.0.9.	2026-08-03	7.5	CVE-2026-69152
kata-containers--kata-containers	Kata Containers is an open source project focusing on a standard implementation of lightweight Virtual Machines (VMs) that perform like containers. Prior to version 4.0.0, kata-runtime is vulnerable to host code execution via an unvalidated configuration path annotation. The runtime accepts an arbitrary io.katacontainers.config_path pod annotation and loads the referenced host TOML file without restriction. As a result, a pod user who can place a file at a host-visible path can supply a configuration that selects an attacker-controlled hypervisor or virtio-fs daemon binary, executing code as root on the host. This issue is fixed in version 4.0.0.	2026-08-07	9.6	CVE-2026-50540
Keysight--Hawkeye	Keysight IxChariot Endpoint and associated products contain a stack-based buffer overflow. An unauthenticated remote attacker can send a specially crafted packet and execute arbitrary code with administrative privileges.	2026-08-04	9.8	CVE-2026-49435
Keysight--IxChariot	Keysight IxChariot Endpoint before 9.5.102 contains a heap-based buffer overflow. An unauthenticated remote attacker can send a specially crafted packet to crash the endpoint or potentially execute arbitrary code.	2026-08-04	9.8	CVE-2017-20241
Keysight--IxChariot	Keysight IxChariot Endpoint before 9.5.102 contains a stack-based buffer overflow. An unauthenticated remote attacker can send a specially crafted packet to crash the endpoint or potentially execute arbitrary code.	2026-08-04	9.8	CVE-2017-20242
keywordrush--Content Egg	The Content Egg - Affiliate Product Importer & Price Comparison plugin for WordPress is vulnerable to Arbitrary File Deletion via Path Traversal in versions up	2026-08-05	8.1	CVE-2026-15979

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Affiliate Product Importer & Price Comparison	to and including 11.3.0. This is due to insufficient validation of the 'img_file' field within the cegg_data post metadata: the value passes only through wp_strip_all_tags() (which does not strip path traversal sequences), is stored directly in post meta, and is later concatenated without normalization into a filesystem path in getFullImgPath() before being passed to PHP's unlink(). This makes it possible for authenticated attackers, with author-level access and above, to delete arbitrary files on the affected site's server which may make remote code execution possible.			
klever-io--klever-go	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.18, the P2P resolver request handling logic is vulnerable to hash-array amplification. A connected peer can send a compressed RequestDataType_HashArrayType direct request that is only 442 bytes on the wire but expands into 200,000 decoded hash entries inside the resolver path. The resolver's antiflood logic counts only a single logical message and the compressed wire size, and while Batch.Decompress() caps the decompressed byte size, it never limits the number of decoded repeated-field items. As a result, both TxResolver and TrieNodeResolver preallocate and iterate over the entire unchecked set of decoded hashes, causing remote memory and CPU amplification against any node that accepts P2P peer connections. This issue is fixed in version 1.7.18.	2026-08-07	7.5	CVE-2026-47249
klever-io--klever-go	Klever-Go is the Go implementation of the Klever blockchain protocol. Versions 1.7.14 through 1.7.17 are vulnerable to a nil-pointer panic triggered by a protobuf Transaction whose embedded RawData sub-message is omitted. This omission causes RawData to decode to nil. Every transaction gossiped on the Klever-Go P2P network is decoded and validated synchronously inside the libp2p pubsub topic-validator callback, where txVersionChecker.CheckTxVersion dereferences tx.RawData.Version with no nil check. Because the libp2p pubsub callback, the underlying go-libp2p-pubsub validation worker, and Klever's own network/p2p layer install no recover(), the panic propagates and crashes the entire node process. The attacker payload is a 3-byte protobuf message; no validator key, stake, funds, or on-chain account is required, and delivery aimed at enough of the BLS validator set can halt block production, resulting in a chain halt. This issue has been fixed in version 1.7.18.	2026-08-07	7.5	CVE-2026-52878
klever-io--klever-go	Klever-Go is the Go implementation of the Klever blockchain protocol. In versions 1.7.14 through 1.7.17, the direct-message ingress handler spawns a new goroutine for every incoming direct message before the processor-level antiflood layer makes any admission decision, with no semaphore, throttler, or bound on the number of concurrent in-flight spawns. Because the antiflood check runs inside the spawned goroutine rather than before it, a single connected peer can open a direct-send stream and send a stream of well-formed messages to force unbounded goroutine creation, where each goroutine allocates its own stack and holds a message reference until processing completes, adding scheduler and garbage-collection pressure faster than the runtime can drain it. This lets one peer degrade the node's availability and its ability to process legitimate traffic, resulting in a remotely triggerable denial of service. The issue is fixed in 1.7.18.	2026-08-07	7.5	CVE-2026-52879
klever-io--klever-go	Klever-Go is the Go implementation of the Klever blockchain protocol. Versions from 1.7.14 through 1.7.17 are vulnerable to a remotely triggerable denial of service. Both REST APIs are started with the Gin Engine.Run convenience method, which serves requests through Go's default HTTP server with no ReadHeaderTimeout, ReadTimeout, or MaxHeaderBytes configured. As a result, incoming connections that never complete their request headers are held open indefinitely. When a REST listener is reachable beyond localhost through the documented all-interface bind or a Docker port-publish deployment, a single unauthenticated client can open many slow-header connections and hold them open until server file descriptors are exhausted, preventing the API from accepting new connections. This renders the REST API unavailable to legitimate clients. This issue is fixed in version 1.7.18.	2026-08-07	7.5	CVE-2026-52880
Koenkk--zigbee2mqtt	Zigbee2MQTT's ExternalJSExtension.getFilePath() (lib/extension/externalJS.ts) joins a `name` parameter received via an MQTT message (topic zigbee2mqtt/bridge/request/extension/save) into the extensions base path using path.join(basePath, name) with no sanitization. Because path.join() resolves `../` sequences, a name such as `../tmp/evil.js` escapes the intended extensions directory. The extension handler only validates that the name ends in .js/.mjs/.cjs, writes the file, and then dynamically imports it via Node.js import(), achieving remote code execution. Requires the `enable_external_js` config option (off by default, but commonly enabled in legacy installs) and MQTT broker access, which is	2026-08-05	8.1	CVE-2026-71279

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	frequently unauthenticated in real deployments. The identical unsanitized <code>getFilePath()</code> is also used by the extension-removal handler, enabling arbitrary file deletion.			
Koha Community--Koha	Koha's reports/acquisitions_stats.pl builds its per-cell statistics query in sub calculate by interpolating the user-controlled Filter request parameters directly into WHERE fragments covering aqbasket.closedate, aqorders.datereceived, aqbooksellers.name, items.homebranch, items.ccode, biblioitems.itemtype, aqbudgets.budget_code, aqorders.sort1, and aqorders.sort2. The statement is prepared and executed with no bound parameters. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), borrower_password_recovery, api_keys, and sessions.	2026-08-04	8.8	CVE-2026-70369
Koha Community--Koha	Koha's reports/catalogue_stats.pl builds dynamic SQL in sub calculate by interpolating the user-controlled Line and Column request parameters directly into identifier positions of the query (SELECT DISTINCTROW, GROUP BY, ORDER BY) with no whitelist validation. When Line contains itemcallnumber and the cotedigits parameter is truthy, cotedigits is additionally concatenated raw as the numeric argument of a LEFT() call. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), api_keys, and sessions.	2026-08-04	8.8	CVE-2026-70370
Koha Community--Koha	Koha's reports/issues_avg_stats.pl builds dynamic SQL in sub calculate by concatenating several user-controlled request parameters directly into the query string. The Line and Column parameters are not validated against any whitelist and land verbatim in identifier positions (SELECT DISTINCTROW, GROUP BY, ORDER BY), and each Filter slot is concatenated raw into single-quoted LIKE, BETWEEN, and comparison fragments with no bound parameters. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), api_keys, and sessions.	2026-08-04	8.8	CVE-2026-70371
Koha Community--Koha	Koha's reports/bor_issues_top.pl builds dynamic SQL in sub calculate by concatenating several user-controlled request parameters directly into the query string. The Criteria parameter is only normalized by a table-name prefix and is never whitelisted, landing verbatim in identifier positions (SELECT DISTINCTROW, GROUP BY, ORDER BY); Filter values are concatenated raw into single-quoted LIKE, BETWEEN, and comparison fragments, and the Limit parameter is appended raw to a LIMIT clause. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), api_keys, and sessions.	2026-08-04	8.8	CVE-2026-70372
Koha Community--Koha	Koha's reports/issues_stats.pl (the circulation statistics report) builds its calculation query in sub calculate by concatenating several user-controlled request parameters directly into the SQL string. The PeriodTypeSel, PeriodDaySel, and PeriodMonthSel parameters are interpolated raw into single-quoted equality and function-comparison fragments, and the Filter slots plus the Line and Column identifiers are likewise interpolated with no whitelist and no placeholder binding. An authenticated staff user holding the reports module permission can inject arbitrary SQL and read any table reachable by the Koha database user, including borrowers (password hashes, two-factor secrets, personal data), api_keys, and sessions.	2026-08-04	8.8	CVE-2026-70373
Koha Community--Koha	Koha's guided report builder (reports/guided_reports.pl) reads the `order_by` CGI parameter and, for each value, a dynamically-named `{order}_ovalue` parameter, and concatenates both directly into an SQL ORDER BY clause with no allowlist or validation: `my @order_by = \$input->multi_param('order_by'); foreach my \$order (@order_by) { my \$value = \$input->param(\$order . "_ovalue"); \$query_orderby = "ORDER BY \$order \$value"; }`. The resulting string is appended verbatim to the final query in C4::Reports::Guided ('\$query .= \$orderby;') with no escaping. Since ORDER BY columns cannot be bound via prepared-statement placeholders, this requires an explicit allowlist, which does not exist. Any staff account with the low-privilege create_reports or execute_reports permission (commonly granted to non-admin library staff) can perform time-based blind SQL injection against the Koha database, which stores patron PII and staff/LDAP credentials.	2026-08-05	8.8	CVE-2026-71288
kosinix--raster	The raster Rust crate's crop() function (src/editor.rs) clamps the crop width/height against source dimensions but only clamps the offset_x/offset_y parameters	2026-08-05	7.5	CVE-2026-71202

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	against 0, never against the source width/height. When an offset exceeds the corresponding source dimension, `width2 - offset_x` (or the height equivalent) underflows to a negative i32, which release builds do not trap; the negative value is then cast to usize inside Image::blank()'s Vec::with_capacity() call, triggering a capacity-overflow panic and crashing the process on a single crafted crop request.			
krayin--laravel-crm	Krayin CRM 2.2.4 contains a missing authentication vulnerability in the installer middleware that allows unauthenticated remote attackers to overwrite the primary administrator account by sending a crafted HTTP POST request with the X-Requested-With: XMLHttpRequest header to bypass the CanInstall middleware redirect check. Attackers can supply arbitrary name, email, and password values to the admin-config-setup endpoint, which performs an unauthenticated updateOrInsert targeting the hardcoded administrator user ID, enabling full administrative access to all CRM data.	2026-08-03	9.8	CVE-2026-41452
krayin--laravel-crm	Krayin CRM before 2.2.4 contains a blind SQL injection vulnerability in the leads DataGrid that allows authenticated users with leads access to inject arbitrary SQL into a HAVING clause by manipulating the rotten_lead[in] query parameter, which is concatenated without parameterized binding directly into a havingRaw() call in LeadDataGrid.php. Attackers can exploit this flaw using time-based and boolean-based blind injection techniques to extract the entire database contents, including user credential hashes, CRM records, and application configuration data.	2026-08-03	8.8	CVE-2026-41453
lattepress--AnsPress Question and answer	Subscriber Broken Access Control in AnsPress - Question and answer 4.4.4 versions.	2026-08-06	7.1	CVE-2026-65554
Leantime--Leantime	Leantime through 3.6.2 exposes the JSON-RPC methods leantime.rpc.TwoFA.TwoFA.getSetupData, saveSecret, verifyAndEnable, and disable2FA, which act on a caller-supplied userId parameter with no ownership check, session pinning, or permission-attribute gate (unlike other RPC-exposed methods in the same dispatcher). Any authenticated user can invoke getSetupData with an arbitrary userId to read that user's live TOTP secret, or disable2FA to strip another account's two-factor authentication entirely, fully defeating account-level 2FA protection. This is related to CVE-2026-15509, which covers a similar missing-authorization pattern in the JSON-RPC editUser/addUser role-assignment path in the same application; the TwoFA service methods addressed here are a distinct, independently fixable set of RPC endpoints.	2026-08-05	8.1	CVE-2026-54418
Lenovo--XClarity Orchestrator	An improper neutralization of special elements used in an operating system command vulnerability was reported in Lenovo XClarity Orchestrator (LXCO) 2.2.0 that could allow an authenticated attacker to execute arbitrary operating system commands as a privileged user under a specific circumstance.	2026-08-04	8.8	CVE-2026-16793
letta-ai--LettaBot	A vulnerability was detected in letta-ai LettaBot 0.2.0. Impacted is an unknown function of the file src/api/server.ts of the component API Status Route. The manipulation results in missing authentication. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	7.3	CVE-2026-18990
lightsyncpro--LightSync Pro Connect & Sync Cloud Assets Lightroom, Canva, Figma, Dropbox & Shutterstock	The LightSync Pro plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the rest_replace_media() function in all versions up to, and including, 2.1.6. This makes it possible for authenticated attackers, with Author-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	2026-08-05	8.8	CVE-2026-6147
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: don't free the ASCONF's own transport in DEL-IP processing sctp_process_asconf() caches the transport the ASCONF chunk is processed against in asconf->transport (== chunk->transport, set once in sctp_rcv()). For an ASCONF located through its Address Parameter by __sctp_rcv_asconf_lookup(), that cached transport corresponds to the Address Parameter, which need not be the packet's source address. sctp_process_asconf_param() rejects a DEL-IP for the packet source address (ADDIP D8, SCTP_ERROR_DEL_SRC_IP), but nothing protects asconf->transport. A single ASCONF can therefore carry, in order: [Address Parameter L] [DEL-IP L] [DEL-IP 0.0.0.0] where L differs from the source. The DEL-IP for L passes the D8 check and calls sctp_assoc_rm_peer() on the transport that asconf->transport still points at, freeing it (RCU-deferred). The following wildcard DEL-IP then reuses the now-dangling asconf->transport in sctp_assoc_set_primary() and sctp_assoc_del_nonprimary_peers(): set_primary() dereferences the freed	2026-08-04	9.8	CVE-2026-64564

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	transport (->ipaddr, ->state) and plants the dangling pointer into asoc->peer.primary_path / active_path, and del_nonprimary_peers(), keeping only the pointer that is no longer on the list, removes every real transport, leaving the association with a transport_count of 0 and primary_path/active_path pointing at freed memory. Reject a DEL-IP that targets the transport the ASCONF is being processed against, mirroring the existing source-address guard, so the wildcard branch can never reuse a freed transport.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: propagate SKBFL_SHARED_FRAG in iptfs_skb_add_frags() When iptfs_skb_add_frags() copies frag references from the source frag walk into a new SKB, it increments the page reference count via __skb_frag_ref() but does not propagate SKBFL_SHARED_FRAG to the destination SKB's skb_shinfo->flags. If the source SKB carries shared frags (e.g. from a page-pool backed receive path), the new inner SKB will appear to ESP as having privately owned frags. A subsequent esp_input() call for a nested transport-mode SA then takes the no-COW fast path and decrypts in place, writing over pages that are still referenced by the outer IPTFS SKB. This causes kernel-visible memory corruption and can trigger a panic. All other frag-transfer helpers in the kernel (skb_try_coalesce, skb_gro_receive, __pskb_copy_fclone, skb_shift, skb_segment) correctly propagate SKBFL_SHARED_FRAG; align iptfs_skb_add_frags() with this convention by setting the flag inside the loop immediately after __skb_frag_ref() and nr_frags++, so every exit path that attaches a frag unconditionally propagates SKBFL_SHARED_FRAG.	2026-08-05	9.8	CVE-2026-64566
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix double-free in SMB2_close() replay A response-bearing attempt can return a replayable error and free its response buffer. If SMB2_close_init() fails before the next send, cleanup retains the previous buffer type and frees that response again. Reset response bookkeeping before each attempt to prevent the stale free.	2026-08-06	9.8	CVE-2026-64597
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Check for invalid/obsolete root *after* making MMU pages available Check for a "stale" page fault, i.e. for an invalid and/or obsolete root, after making MMU pages available for the shadow MMU. If reclaiming shadow pages zaps an in-use root, i.e. marks it invalid, then KVM will attempt to map memory into an invalid root. On its own, populating an invalid root is "fine", but because child shadow pages inherit their parent's role, any children created during the map/fetch will be created as invalid pages, thus violating KVM's invariant that invalid pages are never on the list of active MMU pages. Note, the underlying flaw has existed since KVM first started tracking invalid roots in 2008 (commit 2e53d63acba7, "KVM: MMU: ignore zapped root pagetables"), but the true badness only came along in 2020 (Linux 5.9) with the invariant that invalid shadow pages can't be on the list of active pages. Note #2, inheriting role.invalid when creating child shadow pages is also far from ideal; that flaw will be addressed separately.	2026-08-04	8.8	CVE-2026-64561
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: nVMX: Hide shadow VMCS right after VMCLEAR free_nested() frees the shadow VMCS while vmcs01 still points to it. But because it is asynchronous with respect to loaded_vmcs_clear(), the vCPU might migrate before the pointer is cleared and __loaded_vmcs_clear() may then execute VMCLEAR. The VMCS needs to stay attached until its explicit VMCLEAR completes, but then it can be hidden and the page safely freed.	2026-08-04	8.8	CVE-2026-64562
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate compound request size before reading StructureSize2 When ksmbd validates a compound (chained) SMB2 request, ksmbd_smb2_check_message() reads pdu->StructureSize2 without first checking that the compound element is large enough to contain it. StructureSize2 is a 2-byte field at offset 64 (__SMB2_HEADER_STRUCTURE_SIZE) from the start of each element. The compound-walking logic only guarantees that a full 64-byte SMB2 header is present for the trailing element: when NextCommand is 0, len is reduced to the number of bytes remaining after next_smb2_rcv_hdr_off. A remote client can craft a compound request whose last element has exactly 64 bytes, so the 2-byte StructureSize2 read at offset 64 extends one byte past the receive buffer, producing a slab-out-of-bounds read. BUG: KASAN: slab-out-of-bounds in ksmbd_smb2_check_message (fs/smb/server/smb2misc.c:402) Read of size 2 at addr ffff888012ae31ac by task kworker/0:1/14 The buggy address is located 172 bytes inside of allocated 173-byte region Workqueue: ksmbd-io handle_ksmbd_work Call Trace: ... kasan_report (mm/kasan/report.c:595)	2026-08-05	8.2	CVE-2026-64578

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ksmbd_smb2_check_message (fs/smb/server/smb2misc.c:402) handle_ksmbd_work (fs/smb/server/server.c:119) process_one_work (kernel/workqueue.c:3314) worker_thread (kernel/workqueue.c:3397) kthread (kernel/kthread.c:436) ret_from_fork (arch/x86/kernel/process.c:158) ret_from_fork_asm (arch/x86/entry/entry_64.S:245) Reject any compound element that is too small to hold StructureSize2 before dereferencing it.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: drain bus_reset work on device removal brcmf_fw_crashed() and the debugfs "reset" entry both schedule drvr->bus_reset, whose callback recovers drvr through container_of() and dereferences it. The removal path frees drvr (brcmf_free -> wiphy_free) without draining the work, so a bus_reset callback pending or running during removal can outlive drvr. Cancellation cannot live in brcmf_detach() or brcmf_free(): the work callback reaches teardown through the bus .reset op (PCIe brcmf_pcie_reset -> brcmf_detach; SDIO brcmf_sdio_bus_reset -> brcmf_sdiod_remove -> brcmf_free), so cancelling there would wait for the running work and deadlock. Add a per-bus mutex (bus_reset_lock) and route all arming through brcmf_bus_schedule_reset(), which under the lock skips when the bus is marked removing. Each bus remove entry calls brcmf_bus_cancel_reset_work(), which under the same lock sets removing and cancels the work. Holding the mutex across cancel_work_sync() makes the set-removing + drain step atomic. Every producer reaches the arming path from process context -- the PCIe firmware-halt notification runs in the threaded IRQ handler (brcmf_pcie_isr_thread) and the SDIO hostmail path runs from the data workqueue -- so the mutex is taken only in sleepable contexts. Where applicable the remove entry first stops the firmware-crash producer: on PCIe mask the mailbox and synchronize_irq; on SDIO unregister the bus interrupt and cancel the data worker, which also reports firmware halts through brcmf_fw_crashed(). The mutex is initialized at bus allocation. The SDIO suspend power-off path frees drvr through the same brcmf_sdiod_remove() and takes the same lock; resume re-allows the work only on a successful re-probe. Also guard brcmf_fw_crashed() against a NULL bus_if/drvr: it can fire before brcmf_attach() wires up drvr, and it dereferences drvr (bphy_err/brcmf_dev_coredump) before reaching the arming gate. The bus_reset work is shared across buses, so the drain is applied to every remove path: PCIe (the .reset op introduced by the Fixes commit), SDIO (arms the same work through brcmf_fw_crashed()), and USB (via the debugfs "reset" entry). cancel_work_sync() drains a running or pending bus_reset work item before removal frees drvr, and patch 1/2 makes the scratch-buffer release safe when reset teardown has already released those DMA buffers. This patch fixes the lifetime of the bus_reset work item itself. It does not attempt to address the separate, pre-existing lifetime of the asynchronous firmware completion started by the PCIe reset path. That callback needs its own lifetime/ownership protocol and is being tracked separately. This issue was found by an in-house static analysis tool.	2026-08-06	8.8	CVE-2026-64586
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: smb/client: Fix error code in smb2_aead_req_alloc() The "*num_sgs" variable is a u32 so "ERR_PTR(*num_sgs)" doesn't work. We would have to do something similar to the previous line where it's cast to int and then long. However, it's simpler to store the return in an int ret variable. This bug would eventually result in a crash when dereference the invalid error pointer.	2026-08-06	8.8	CVE-2026-64598
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rhashtable: clear stale iter->p on table restart rhashtable_walk_start_check() has two restart paths when resuming a walk. When iter->walker.tbl is valid, it re-validates iter->p against the table and sets iter->p = NULL if the object is gone. When iter->walker.tbl is NULL (table was freed during resize), it resets slot and skip but forgets to clear iter->p. rhashtable_walk_next() then dereferences the stale iter->p, reading freed memory. This is a use-after-free. Any caller that does multi-fragment rhashtable walks across walk_stop/walk_start boundaries is affected. Concrete cases include netlink_diag (__netlink_diag_dump in net/netlink/diag.c) and TIPC (tipc_nl_sk_walk in net/tipc/socket.c). Crash stack (netlink_diag): BUG: KASAN: slab-use-after-free in rhashtable_walk_next+0x365/0x3c0 Read of size 8 at addr ffff88801a9d2438 (freed kmalloc-2k, offset 1080) Call Trace: rhashtable_walk_next+0x365/0x3c0 (lib/rhashtable.c:1016) __netlink_diag_dump+0x160/0x760 (net/netlink/diag.c:122) netlink_diag_dump+0xc2/0x240 netlink_dump+0x5bc/0x1270 netlink_recvmmsg+0x7a3/0x980 sock_recvmmsg+0x1bc/0x200 __sys_recvfrom+0x1d4/0x2c0	2026-08-04	7.8	CVE-2026-64563

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: reject free space cache with more entries than pages When loading a v1 free space cache, __load_free_space_cache() takes num_entries and num_bitmaps straight from the on-disk btrfs_free_space_header. That header is stored in the tree_root under a key with type 0, which the tree-checker has no case for, so neither count is validated before the load trusts it. The load loops num_entries times and maps the next page whenever the current one runs out, going through io_ctl_check_crc() -> io_ctl_map_page(), which does io_ctl->pages[io_ctl->index++]. But pages[] is allocated in io_ctl_init() from the cache inode's i_size, not from num_entries: num_pages = DIV_ROUND_UP(i_size_read(inode), PAGE_SIZE); io_ctl->pages = kcalloc(num_pages, sizeof(struct page *), GFP_NOFS); So if num_entries claims more records than the pages can hold, io_ctl->index runs off the end of pages[]. The write side never hits this because io_ctl_add_entry() and io_ctl_add_bitmap() both stop once io_ctl->index >= io_ctl->num_pages; the read side just never had the same check. To trigger it, take a clean cache (num_entries = <N> here), set num_entries in the header to 0x10000, and fix up the leaf checksum so it still passes the tree-checker. The cache inode has i_size = 65536, so num_pages is 16 and pages[] is a 16-pointer (kmallocc-128) array. The load now tries to read 65536 entries, io_ctl->index walks up to 16, and pages[16] is read past the array: BUG: KASAN: slab-out-of-bounds in io_ctl_check_crc (fs/btrfs/free-space-cache.c:420 fs/btrfs/free-space-cache.c:565) Read of size 8 at addr ffff88800c833a80 by task kworker/u8:3/58 io_ctl_check_crc (fs/btrfs/free-space-cache.c:420 fs/btrfs/free-space-cache.c:565) __load_free_space_cache (fs/btrfs/free-space-cache.c:655 fs/btrfs/free-space-cache.c:820) load_free_space_cache (fs/btrfs/free-space-cache.c:1017) caching_thread (fs/btrfs/block-group.c:880) btrfs_work_helper (fs/btrfs/async-thread.c:312) process_one_work worker_thread kthread ret_from_fork free-space-cache.c:420 is io_ctl_map_page(), inlined into io_ctl_check_crc() at line 565, which is why that is the frame KASAN names. The out-of-bounds slot is then treated as a struct page and handed to crc32c(), so the bad read turns into a GP fault. Add the missing check to io_ctl_check_crc(), which is where both the entry loop and the bitmap loop end up. When num_entries is too large the load now fails like any corrupt cache: __load_free_space_cache() drops it and rebuilds the free space from the extent tree, so a valid cache is never rejected.	2026-08-05	7.8	CVE-2026-64567
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix unsol_bcast_probe_resp double free on alloc failure ieee80211_set_unsol_bcast_probe_resp() calls kfree_rcu() on the old template before allocating the replacement. If the kzalloc() then fails, it returns -ENOMEM while link->u.ap.unsol_bcast_probe_resp still points at the object already queued for freeing. A later update or AP teardown re-queues that same rcu_head; the second free is caught by KASAN when the RCU sheaf is processed in softirq: BUG: KASAN: double-free in rcu_free_sheaf (mm/slub.c:5850) Free of addr ffff88800d06f300 by task exploit/145 ... __rcu_free_sheaf_prepare (mm/slub.c:2634 mm/slub.c:2940) rcu_free_sheaf (mm/slub.c:5850) rcu_core (kernel/rcu/tree.c:2617 kernel/rcu/tree.c:2869) handle_softirqs (kernel/softirq.c:622) The buggy address belongs to the cache kmalloc-128 of size 128 Queue the old object for kfree_rcu() only after the new one is published, matching ieee80211_set_probe_resp() and ieee80211_set_s1g_short_beacon().	2026-08-05	7.8	CVE-2026-64568
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix fils_discovery double free on alloc failure ieee80211_set_fils_discovery() calls kfree_rcu() on the old template before allocating the replacement. If the kzalloc() then fails, it returns -ENOMEM while link->u.ap.fils_discovery still points at the object already queued for freeing. A later update or AP teardown (ieee80211_stop_ap()) re-queues that same rcu_head; the second free is caught by KASAN when the RCU sheaf is processed in softirq: BUG: KASAN: double-free in rcu_free_sheaf (mm/slub.c:5850) Free of addr ffff88800c065280 by task swapper/0/0 ... __rcu_free_sheaf_prepare (mm/slub.c:2634 mm/slub.c:2940) rcu_free_sheaf (mm/slub.c:5850) rcu_core (kernel/rcu/tree.c:2617 kernel/rcu/tree.c:2869) handle_softirqs (kernel/softirq.c:622) The buggy address belongs to the cache kmalloc-96 of size 96 Queue the old object for kfree_rcu() only after the new one is published, matching ieee80211_set_probe_resp() and ieee80211_set_s1g_short_beacon().	2026-08-05	7.8	CVE-2026-64570
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: tear down new links on vif update error path When ieee80211_vif_update_links() adds new links it allocates a link container for each and calls ieee80211_link_init() (which registers the per-link debugfs files with file->private_data pointing into the	2026-08-05	7.8	CVE-2026-64574

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	container) and ieee80211_link_setup(). If the subsequent drv_change_vif_links() fails, the error path restores the old pointers and jumps to 'free', which frees the new containers but never removes their debugfs entries or stops the links. The debugfs files survive with file->private_data dangling at the freed container, so a later open()+read() (e.g. link-1/txpower) dereferences freed memory in ieee80211_if_read_link(), a use-after-free. The removal path already dismantles links correctly via ieee80211_tear_down_links(), which removes each link's keys and debugfs entries and calls ieee80211_link_stop(); the add path on the error branch does not. Commit be1ba9ed221f ("wifi: mac80211: avoid weird state in error path") hardened this same error path for the link-removal case (new_links == 0) but left the newly-added links' teardown unaddressed. drv_change_vif_links() can fail at runtime on MLO drivers (internal allocation / queue / firmware command failures). Remove the new links' debugfs entries and stop them before freeing. BUG: KASAN: slab-use-after-free in ieee80211_if_read_link (net/mac80211/debugfs_netdev.c:127) Read of size 8 at addr ffff888011290000 by task exploit/145 Call Trace: ... ieee80211_if_read_link (net/mac80211/debugfs_netdev.c:127) short_proxy_read (fs/debugfs/file.c:373) vfs_read (fs/read_write.c:572) ksys_read (fs/read_write.c:716) do_syscall_64 (arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) ... Oops: general protection fault, probably for non-canonical address 0xdffffc000000000a RIP: 0010:ieee80211_if_read_link (net/mac80211/debugfs_netdev.c:127) Kernel panic - not syncing: Fatal exception			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: tcp: fix double sock release on batch realloc bpf_iter_tcp_batch() releases the current batch via bpf_iter_tcp_put_batch(), which drops the socket refs and rewrites each slot with the socket cookie, then grows the batch. cur_sk/end_sk are kept for bpf_iter_tcp_resume(), but on realloc failure the function returns ERR_PTR() before resume runs, leaving cur_sk < end_sk over slots that now hold cookies rather than sock pointers. bpf_iter_tcp_seq_stop() then calls bpf_iter_tcp_put_batch() again and dereferences a cookie as a struct sock. Empty the batch on the failure path so stop() does not release it again. The sockets were already freed by the first bpf_iter_tcp_put_batch(), so nothing leaks, and a later read() rescans the bucket from the start instead of skipping it. The sibling GFP_NOWAIT failure path still holds real socket references and is left for stop() to release. BUG: KASAN: null-ptr-deref in __sock_gen_cookie Read of size 8 at addr 0000000000000059 by task exploit ... __sock_gen_cookie (net/core/sock_diag.c:28) bpf_iter_tcp_put_batch (net/ipv4/tcp_ipv4.c:2918) bpf_iter_tcp_seq_stop (net/ipv4/tcp_ipv4.c:3270) bpf_seq_read (kernel/bpf/bpf_iter.c:205) vfs_read (fs/read_write.c:572) ksys_read (fs/read_write.c:716) do_syscall_64 entry_SYSCALL_64_after_hwframe Kernel panic - not syncing: Fatal exception	2026-08-05	7.8	CVE-2026-64575
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nexthop: initialize extack in nh_res_bucket_migrate() nh_res_bucket_migrate() passes an uninitialized netlink_ext_ack to call nexthop_res_bucket_notifiers(). When nh_notifier_res_bucket_info_init() fails (e.g. the kzalloc returns -ENOMEM), the error is propagated back before any notifier sets extack._msg, and the error path formats the stale pointer with pr_err_ratelimited("%s\n", extack._msg). With CONFIG_INIT_STACK_NONE this dereferences uninitialized stack memory: Oops: general protection fault, probably for non-canonical address ... KASAN: maybe wild-memory-access in range [...] RIP: 0010:string (lib/vsprintf.c:730) vsnprintf (lib/vsprintf.c:2945) _printk (kernel/printk/printk.c:2504) nh_res_bucket_migrate (net/ipv4/nexthop.c:1816) nh_res_table_upkeep (net/ipv4/nexthop.c:1866) rtm_new_nexthop (net/ipv4/nexthop.c:3323) rtnetlink_rcv_msg (net/core/rtnetlink.c:7076) netlink_sendmsg (net/netlink/af_netlink.c:1900) Kernel panic - not syncing: Fatal exception Zero-initialize extack so _msg is NULL on error paths that never set it.	2026-08-05	7.1	CVE-2026-64576
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gtp: check skb_pull_data() return in gtp1u_send_echo_resp() gtp1u_send_echo_resp() ignores skb_pull_data()'s return value. Its caller gtp1u_udp_encap_rcv() only guarantees 16 bytes (udphdr + gtp1_header), but the pull requests 20 (gtp1_header_long + udphdr). For a 16-19 byte echo request the pull fails and returns NULL without advancing skb->data; execution continues, and the following skb_push() plus the IP header pushed by iptunnel_xmit() move skb->data below skb->head, tripping skb_under_panic(). Fix it by dropping the packet when skb_pull_data() fails. skbuff: skb_under_panic: ... kernel BUG at	2026-08-05	7.5	CVE-2026-64577

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	net/core/skbuff.c:214! Call Trace: skb_push (net/core/skbuff.c:2648) iptunnel_xmit (net/ipv4/ip_tunnel_core.c:82) gtp_encap_rcv (drivers/net/gtp.c:701 drivers/net/gtp.c:808 drivers/net/gtp.c:920) udp_queue_rcv_one_skb (net/ipv4/udp.c:2388) ... Kernel panic - not syncing: Fatal exception in interrupt			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm6: clear dst.dev on error to avoid double netdev_put in xfrm6_fill_dst() On the error path where in6_dev_get(dev) returns NULL, xfrm6_fill_dst() releases the device reference with netdev_put() but leaves xdst->u.dst.dev set. dst_destroy() later calls netdev_put(dst->dev) again, so the same net_device reference is released twice, underflowing its refcount (ref_tracker WARNING + "unregister_netdevice: waiting for <dev> to become free"). Clear xdst->u.dst.dev after the netdev_put(), the same way the XFRM device-offload paths xfrm_dev_state_add() and xfrm_dev_policy_add() in net/xfrm/xfrm_device.c NULL ->dev when releasing the reference on error. ref_tracker: reference already released. ref_tracker: allocated in: xfrm6_fill_dst (net/ipv6/xfrm6_policy.c:86) ... udpv6_sendmsg (net/ipv6/udp.c:1696) ... ref_tracker: freed in: xfrm6_fill_dst (net/ipv6/xfrm6_policy.c:90) ... WARNING: lib/ref_tracker.c:322 at ref_tracker_free+0x58b/0x780 dst_destroy (net/core/dst.c:115) rcu_core handle_softirqs ...	2026-08-05	7.8	CVE-2026-64580
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: fix sk_dst_cache double-free in xfrm_user_policy() xfrm_user_policy() clears the socket dst cache with __sk_dst_reset(), i.e. the non-atomic __sk_dst_set(sk, NULL): it reads sk_dst_cache with rcu_dereference_protected(), stores NULL and dst_release()s the old dst. That is only safe if no other thread modifies sk_dst_cache concurrently. For a connected UDP socket that does not hold: the transmit fast path (udp_sendmsg -> sk_dst_check -> sk_dst_reset) resets the cache locklessly with an atomic xchg(). A per-socket policy change racing a send can make both sides observe the same old dst and each dst_release() it, dropping the socket's single reference twice and freeing the xfrm_dst bundle while it is still referenced: BUG: KASAN: slab-use-after-free in dst_release Write of size 4 at addr ffff88801897b6c0 by task exploit/155 Call Trace: ... dst_release (... ./include/linux/rcuref.h:109) xfrm_user_policy (./include/net/sock.h:2239 ./include/net/sock.h:2256 net/xfrm/xfrm_state.c:3053) do_ip_setsockopt (net/ipv4/ip_sockglue.c:1347) ip_setsockopt (net/ipv4/ip_sockglue.c:1417) do_sock_setsockopt (net/socket.c:2368) __sys_setsockopt (net/socket.c:2393) _x64_sys_setsockopt (net/socket.c:2396) do_syscall_64 (arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) Reachable by an unprivileged user via a user+network namespace. Use the atomic sk_dst_reset() so the cache is cleared and released with a single xchg(): whichever side wins releases the dst once, the other sees NULL and does nothing. Behaviour is otherwise unchanged.	2026-08-05	7.8	CVE-2026-64581
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix a use-after-free problem in rxe_mmap rxe_mmap() removes a rxe_mmap_info struct from the pending_mmmaps list and releases pending_lock while the struct's kref is still at 1: list_del_init(&ip->pending_mmmaps); spin_unlock_bh(&rxe->pending_lock); /* ref == 1, no lock held */ ret = remap_vmalloc_range(vma, ip->obj, 0); /* walks PTEs */ [...] rxe_vma_open(vma); /* kref_get, ref Ã¢â 2 */ remap_vmalloc_range_partial() walks PTEs without any lock. A concurrent DESTROY_CQ ioctl on another CPU calls: kref_put(&q->ip->ref, rxe_mmap_release) /* ref 1Ã¢â 0 */ vfree(ip->obj) /* clears vmalloc PTEs mid-walk */ kfree(ip) /* frees rxe_mmap_info */ This yields: 1. Kernel crash, vmalloc_to_page() returns NULL when vfree wins the per-PTE race -> vm_insert_page(NULL) Ã¢â GPF in validate_page_before_insert 2. Page UAF, vmalloc_to_page() reads a stale PTE before vfree clears it. User VMA holds a PTE to a free'd page which might eventually get reallocated later by vmalloc which allows the attacker to get a clean page-level UAF. It is worth noting that even though a page-level UAF is possible given the strong primitive, it is statistically very difficult to achieve given the very short time window (after the last insert_page and before the kref_get). The call trace are as below: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000001: 0000 [#1] SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000008-0x000000000000000f] CPU: 0 UID: 1000 PID: 413 Comm: poc Not tainted 7.0.0-rc5-dirty #28 PREEMPT(lazy) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:validate_page_before_insert+0x32/0x300 Code: e5 41 57 41 56 49 89 fe 41 55 41 54 53 48 89 f3 e8 93 b5 a3 ff 48 8d 7b 08 48 b8 00 00 00 00 fc ff df 48 89	2026-08-05	7.8	CVE-2026-64582

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	<pre> fa 48 c1 ea 03 <80> 3c 02 00 0f 85 7b 02 00 00 4c 8b 63 08 31 ff 4d 89 e5 41 83 e5 RSP: 0018:ffff8881b15f2f0 EFLAGS: 00000202 RAX: dffffc0000000000 RBX: 0000000000000000 RCX: 0000000000000000 RDX: 0000000000000001 RSI: 0000000000000000 RDI: 0000000000000008 RBP: ffff8881b15f318 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffff8881181eee00 R13: 0000000000000000 R14: ffff8881181eee00 R15: ffff8881181eee20 FS: 00007b1e000f76c0(0000) GS:ffff8884268e0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CRO: 0000000080050033 CR2: 00007b1e00a24ac0 CR3: 0000000116eb3000 CR4: 000000000000006f0 Call Trace: <TASK> insert_page+0x8f/0x190 ? __pfx_insert_page+0x10/0x10 ? kasan_save_alloc_info+0x38/0x60 vm_insert_page+0x2e7/0x400 remap_vmalloc_range_partial+0x212/0x3e0 remap_vmalloc_range+0x6e/0xb0 ? __kasan_check_write+0x14/0x30 rxm_mmap+0x2e9/0x5d0 ib_uverbs_mmap+0x1ad/0x2c0 __mmap_region+0x12c2/0x2ad0 ? __pfx__mmap_region+0x10/0x10 ? __sanitizer_cov_trace_switch+0x58/0xb0 ? mas_prev_slot+0x360/0x39c0 ? __sanitizer_cov_trace_switch+0x58/0xb0 ? mas_next_slot+0x1e5b/0x2f40 ? __sanitizer_cov_trace_cmp8+0x18/0x30 ? unmapped_area_topdown+0x4dd/0x610 ? kfree+0x1b1/0x440 ? free_cpumask_var+0x16/0x30 ? __kasan_slab_free+0x7d/0xa0 ? __sanitizer_cov_trace_cmp8+0x18/0x30 mmap_region+0x2e6/0x3c0 do_mmap+0xa3e/0x12a0 ? __pfx_do_mmap+0x10/0x10 ? __kasan_check_write+0x14/0x30 ? down_write_killable+0xba/0x160 ? __pfx_down_write_killable+0x10/0x10 ? __sanitizer_cov_trace_cmp4+0x16/0x30 vm_mmap_pgoff+0x2d4/0x4a0 ? __pfx_vm_mmap_pgoff+0x10/0x10 ? fget+0x1bf/0x270 ksys_mmap_pgoff+0x40c/0x690 ? __sanitizer_cov_trace_const_cmp4+0x16/0x30 ? __pfx_ksys_mmap_pgoff+0x10/0x10 ? __kasan_check_write+0x14/0x30 ? __raw_spin_trylock+0xbb/0x130 ? __pfx__raw_spin_trylock+0x10/0x10 x64_sys_mmap+0x135/0x1e0 x64_sys_c ---truncated---</pre>			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: udc: bdc: free IRQ and drain func_wake_notify before teardown The Broadcom BDC UDC driver registers its IRQ handler with devm_request_irq() in bdc_udc_init(), so the IRQ is released by devm only after bdc_remove() returns. devm releases resources in reverse LIFO order, but bdc_remove() runs bdc_udc_exit() and bdc_hw_exit() -> bdc_mem_free() manually before returning: bdc_udc_exit() tears down individual endpoint objects via bdc_free_ep(), while bdc_hw_exit() -> bdc_mem_free() frees and NULLs the DMA-coherent status-report ring (bdc->srr.sr_bds) and kfree()s bdc->bdc_ep_array. Both happen while the IRQ handler (bdc_udc_interrupt, requested with IRQF_SHARED) remains deliverable in the window up to the post-remove devm free_irq(). On receipt of a shared interrupt in that window, bdc_udc_interrupt() dereferences bdc->srr.sr_bds[bdc->srr.dqp_index] (NULL or freed DMA) and dispatches sr_handler callbacks that index into bdc_ep_array, causing a NULL-deref or use-after-free. The same window affects the delayed_work bdc->func_wake_notify, which is armed from the IRQ handler via bdc_sr_uspc() -> handle_link_state_change() -> schedule_delayed_work() and may self-rearm from its own callback bdc_func_wake_timer(). No cancel exists anywhere in the driver, so a queued work item that fires after bdc_remove() returns and the bdc structure is devm-freed dereferences freed memory. Replace devm_request_irq() with request_irq() and add an explicit free_irq(bdc->irq, bdc) in bdc_remove(). Clear BDC_GIE before free_irq() to stop the device from asserting interrupts, then free_irq() drains any in-flight handler, then cancel_delayed_work_sync() drains the func_wake_notify delayed work. This ordering ensures the IRQ handler and delayed work cannot interfere with the subsequent endpoint and DMA teardown in bdc_udc_exit() and bdc_hw_exit(). Wire the matching free_irq() into the bdc_udc_init() error path so the IRQ is released on probe failure, and route the bdc_init_ep() failure through err0 instead of returning directly. This issue was found by an in-house static analysis tool.	2026-08-06	7.8	CVE-2026-64583
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_midi: cancel pending IN work before freeing the midi object The f_midi driver embeds a work item (midi->work) whose handler, f_midi_in_work(), dereferences the enclosing struct f_midi through container_of(). This work is armed from two sites: f_midi_complete(), on a normal IN-endpoint completion, and f_midi_in_trigger(), on an ALSA rawmidi output-stream start. Neither	2026-08-06	7.8	CVE-2026-64584

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	f_midi_disable() nor f_midi_unbind() cancels midi->work. f_midi_disable() only disables the endpoints and drains the in_req_fifo; it does not synchronize the work item, and the sound card is released asynchronously to the final free of the midi object. The midi object is reference-counted (midi->free_ref) and is freed in f_midi_free() only once both the usb_function reference and the rawmidi private_data reference have been dropped. In f_midi_unbind(), f_midi_disable() runs before the sound card is released, so while the USB endpoints are already disabled the rawmidi device is still usable by an open substream. A concurrent userspace write on such a substream can reach f_midi_in_trigger() and queue midi->work again after f_midi_disable() has returned. A work item armed this way may still be pending when the last reference drops and f_midi_free() proceeds to kfree(midi), letting f_midi_in_work() dereference the struct after it has been freed, a use-after-free. For this reason cancelling midi->work in f_midi_disable() would not be sufficient: the ALSA trigger path can rearm the work after disable() returns. Cancelling at the refcount-zero free site is the boundary after which neither arming source can survive, because by then both references that keep the midi object alive have been dropped: the USB endpoints are already disabled and the rawmidi device has been released. Fix this by calling cancel_work_sync(&midi->work) in the refcount-zero block of f_midi_free(), before the embedded work_struct is freed along with the rest of the structure. opts->lock is a sleeping mutex, so calling cancel_work_sync() under it is permitted, and the handler takes midi->transmit_lock rather than opts->lock, so no self-deadlock can occur while it waits for a running instance of the work to finish. This issue was found by an in-house static analysis tool.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: esd_usb: kill anchored URBs before freeing netdevs esd_usb_disconnect() frees each CAN netdev with free_candev() inside its per-netdev loop and only calls unlink_all_urbs(dev) afterwards. The per-netdev private data (struct esd_usb_net_priv) is embedded in the net_device allocation returned by alloc_candev(), so once free_candev() has run, dev->nets[i] points to freed memory. unlink_all_urbs() then dereferences the freed dev->nets[i] to kill the per-netdev TX anchor (usb_kill_anchored_urbs(&priv->tx_submitted)), clear active_tx_jobs, and reset priv->tx_contexts[]. Reorder the teardown so the anchored URBs are killed before the netdevs are freed, matching other CAN/USB drivers in the same directory such as ems_usb, usb_8dev and mcba_usb, which unregister, then unlink, then free: unregister the netdevs first (which stops their TX queues), call unlink_all_urbs(dev) once, then free the netdevs. This issue was found by an in-house static analysis tool.	2026-08-06	7.8	CVE-2026-64585
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: arc: emac: quiesce interrupts before requesting IRQ Normal RX/TX interrupts are enabled later, in arc_emac_open(), so probe should not see interrupt delivery in the usual case. However, hardware may still present stale or latched interrupt status left by firmware or the bootloader. If probe later unwinds after devm_request_irq() has installed the handler, such a stale interrupt can still reach arc_emac_intr() during teardown and race with release of the associated net_device. Avoid that window by putting the device into a known quiescent state before requesting the IRQ: disable all EMAC interrupt sources and clear any pending EMAC interrupt status bits. This keeps the change hardware-focused and minimal, while preventing spurious IRQ delivery from leftover state.	2026-08-06	7	CVE-2026-64587
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fuse-uring: fix data races on ring->ready On weakly-ordered architectures, the store to fiq->ops can be reordered past the store to ring->ready, allowing a CPU that sees ring->ready == true via fuse_uring_ready() to dispatch requests through a stale fiq->ops pointer. Upgrade the store to smp_store_release() and the load in fuse_uring_ready() to smp_load_acquire() so that the preceding WRITE_ONCE(fiq->ops, ...) is visible to any CPU that observes ring->ready == true. Additionally, fuse_uring_do_register() publishes ring->ready with WRITE_ONCE() but the fast-path check reads it with a plain load. This is a marked-vs-unmarked access that KCSAN will flag. Wrap it in READ_ONCE() to mark it without adding unnecessary ordering. Also wrap the fc->ring load in fuse_uring_ready() in READ_ONCE() to prevent the compiler from reloading it between the NULL check and the dereference.	2026-08-06	7.8	CVE-2026-64588
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: amlogic - avoid double cleanup in meson_crypto_probe() When meson_allocate_chanlist() fails after a partial allocation, it already unwinds the allocated chanlist state	2026-08-06	7.8	CVE-2026-64599

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	through its local error path. meson_crypto_probe() then jump to error_flow and calls meson_free_chanlist() again, causing the same per-flow resources to be torn down twice. In the reproduced failure path, the second teardown re-entered crypto_engine_exit() on an already destroyed worker and KASAN reported a slab-use-after-free in kthread_destroy_worker(). Prevent double-free by handling partial allocation failures locally within meson_allocate_chanlist() and skipping the outer cleanup path. The bug was first flagged by an experimental analysis tool we are developing for kernel memory-management bugs while analyzing v6.13-rc1. The tool is still under development and is not yet publicly available. The bug was reproduced in a QEMU x86_64 guest booted with KASAN on v7.1, using the reproducer under tools/testing/meson_crypto_probe. The reproducer forces the second dma_alloc_attrs() call in the gxl-crypto probe path to return NULL, making meson_allocate_chanlist() fail after partial initialization. On the unpatched kernel this reliably triggered a slab-use-after-free. With this fix applied, the same reproducer no longer emits any KASAN report and the probe fails cleanly with -ENOMEM. ===== BUG: KASAN: slab-use-after-free in kthread_destroy_worker+0xb2/0xd0 Read of size 8 at addr ff1100010c057a68 by task insmod/265 CPU: 1 UID: 0 PID: 265 Comm: insmod Tainted: G O 7.1.0-rc2-00376-g810af9adc907-dirty #10 PREEMPT(lazy) Tainted: [O]=OOT_MODULE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x68/0xa0 print_report+0xcb/0x5e0 ? __virt_addr_valid+0x21d/0x3f0 ? kthread_destroy_worker+0xb2/0xd0 ? kthread_destroy_worker+0xb2/0xd0 kasan_report+0xca/0x100 ? kthread_destroy_worker+0xb2/0xd0 kthread_destroy_worker+0xb2/0xd0 meson_crypto_probe+0x4d0/0xc10 [amlogic_gxl_crypto] platform_probe+0x99/0x140 really_probe+0x1c6/0x6a0 ? __pfx__device_attach_driver+0x10/0x10 __driver_probe_device+0x248/0x310 ? acpi_driver_match_device+0xb0/0x100 driver_probe_device+0x48/0x210 ? __pfx__device_attach_driver+0x10/0x10 __device_attach_driver+0x160/0x320 bus_for_each_drv+0x104/0x190 ? __pfx_bus_for_each_drv+0x10/0x10 ? __raw_spin_unlock_irqrestore+0x2c/0x50 __device_attach+0x19d/0x3b0 ? __pfx__device_attach+0x10/0x10 ? do_raw_spin_unlock+0x53/0x220 device_initial_probe+0x78/0xa0 bus_probe_device+0x5b/0x130 device_add+0xcfd/0x1430 ? __pfx_device_add+0x10/0x10 ? insert_resource+0x34/0x50 ? lock_release+0xc9/0x290 platform_device_add+0x24e/0x590 ? __pfx_meson_crypto_probe_repro_init+0x10/0x10 [meson_crypto_probe_repro] meson_crypto_probe_repro_init+0x330/0xff0 [meson_crypto_probe_repro] do_one_initcall+0xc0/0x450 ? __pfx_do_one_initcall+0x10/0x10 ? __raw_spin_unlock_irqrestore+0x2c/0x50 ? __create_object+0x59/0x80 ? kasan_unpoison+0x27/0x60 do_init_module+0x27b/0x7d0 ? __pfx_do_init_module+0x10/0x10 ? kasan_quarantine_put+0x84/0x1d0 ? kfree+0x32c/0x510 ? load_module+0x561e/0x5ff0 load_module+0x54fe/0x5ff0 ? __pfx_load_module+0x10/0x10 ? security_file_permission+0x20/0x40 ? kernel_read_file+0x23d/0x6e0 ? mmap_region+0x235/0x4a0 ? __pfx_kernel_read_file+0x10/0x10 ? __file_has_perm+0x2c0/0x3e0 init_module_from_file+0x158/0x180 ? __pfx_init_module_from_file+0x10/0x10 ? __lock_acquire+0x45a/0x1ba0 ? idempotent_init_module+0x315/0x610 ? lock_release+0xc9/0x290 ? lock ---truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: us144mkii: capture_urb_complete: redundant usb_anchor_urb corrupts anchor list on each resubmission In capture_urb_complete(), usb_anchor_urb() is called on every completion callback, but the URB is already anchored from the initial submission in tascam_trigger_start(). Each redundant call corrupts the anchor's doubly-linked list and inflates the URB refcount. When usb_kill_anchored_urbs() traverses the list during stream stop / suspend / disconnect, the corrupted list leads to use-after-free. Remove the redundant usb_anchor_urb() from the resubmit path.	2026-08-06	7.8	CVE-2026-64601
Loca Software Informatics Technology Ltd. Co.--CMS	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Loca Software Informatics Technology Ltd. Co. CMS allows SQL Injection. This issue affects CMS: through 06082026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	9.8	CVE-2026-5134
louislam--uptime-kuma	Uptime Kuma's Matomo analytics integration (server/analytics/matomo-analytics.js) injects the admin-configurable Matomo `siteId` value as a bare, unquoted JavaScript expression inside a <script> block rendered on every public	2026-08-05	8.1	CVE-2026-71285

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	status page: `_paq.push(['setSiteId', `\${escapedSiteIdHTMLAttribute}]);`. The escaping pipeline used (jesc with isScriptContext:true, then html-escaper.escape()) does not escape the characters `]`, `)`, `;`, `(`, which are sufficient to break out of the array/push expression context. A siteId value such as `1));alert(document.cookie)//`, once saved by an editor/admin, executes arbitrary JavaScript for every unauthenticated visitor of the public /status/<slug> page, enabling session-cookie theft and full page takeover.			
LUCID Vision Labs--Arena SDK	DLL Search Order Hijacking in LUCID Vision Labs Arena SDK 1.0.80.49 on Windows allows a local attacker to execute arbitrary code with the privileges of the application by placing a malicious DLL in a user-controlled directory listed in the PATH environment variable, which the SDK traverses when a required dependency is not found locally.	2026-08-07	8.8	CVE-2026-9169
lyric777--Book-Management-System	Book-Management-System's Flask API endpoints /student, /record, /books, /find_stu_book, and /find_not_return_book are missing the @login_required decorator that protects sibling routes (/search_student, /storage) in the same file. This allows any unauthenticated remote user to retrieve student PII (name, gender, card validity, debt status) and full book-borrowing history by supplying a card_id. Because card_id values are sequential integers, the entire student database can be enumerated without authentication.	2026-08-05	7.5	CVE-2026-71241
mackron--dr_libs	dr_libs dr_wav.h (all versions through current master) contains an integer overflow in W64 CUE chunk metadata parsing. In drwav__metadata_process_chunk(), a stage-1 capacity estimate truncates the 64-bit W64 chunk sizeInBytes to size_t before dividing by DRWAV_CUE_POINT_BYTES; on 32-bit builds this truncation causes the pre-allocated extra metadata capacity to be computed incorrectly. The subsequent read in drwav__read_cue_to_metadata_obj() computes the actual cue point count and allocation size using the full-precision, attacker-controlled cuePointCount field without cross-checking it against the stage-1 capacity estimate, and the only bounds enforcement on the resulting memory region (drwav__metadata_get_memory()) is a DRWAV_ASSERT, which compiles to a no-op under -DNDEBUG (the default for release builds). A crafted W64 WAV file can therefore cause a heap buffer overflow in any 32-bit application parsing untrusted WAV metadata.	2026-08-05	7.8	CVE-2026-71261
magicblack--maccms10	MacCMS10's admin template editor (application/admin/controller/Template.php) blocks dangerous PHP functions in template content via a blacklist regex, but the blacklist omitted exec, passthru, popen, show_source, create_function, register_shutdown_function, register_tick_function, and error_log. Combined with ThinkPHP's {if} template tag, which embeds the condition attribute directly into raw PHP (<?php if(condition): ?>), an authenticated administrator could inject a payload such as {if condition="exec('id > /tmp/pwned.txt')} to achieve remote code execution. Fixed in commit 71ad3bb29570e110d8e973acff68040a3050ddf0 (2026-06-22), which added the missing functions to the filter.	2026-08-05	7.2	CVE-2026-71232
mailmunch--Mailmunch Forms for Mailchimp	The MailChimp Forms by MailMunch plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `sign_in()` and `sign_up()` AJAX handlers in all versions up to, and including, 3.2.7. This makes it possible for authenticated attackers, with Subscriber-level access and above, to relink the site's MailMunch integration to an attacker-controlled MailMunch account by submitting attacker-supplied credentials. Once relinked, all subscriber data captured by the plugin's forms is delivered to the attacker, and the forms/landing pages rendered on the site are pulled from the attacker's MailMunch account.	2026-08-05	8.1	CVE-2026-7520
mautic--mautic	Mautic's getLeadIdsByFieldValueAction (LeadBundle/Controller/AjaxController.php) reads a field parameter from the request, sanitizes it only with InputHelper::clean() (which HTML-entity-encodes quotes and angle brackets but does not restrict other characters), and passes it into LeadRepository::buildQueryForGetLeadsByFieldValue() where it is concatenated directly as a raw SQL column identifier (\$col = 'I.'. \$field) rather than being validated against a whitelist of real column names or passed as a bound parameter. Since Doctrine cannot parameterize identifiers, and the sanitizer does not block spaces, parentheses, or other SQL-relevant characters, an attacker can inject SQL via the field name itself. The action requires only a valid session (any authenticated user), unlike sibling actions in the same controller that carry additional permission checks.	2026-08-05	7.1	CVE-2026-71245
mawww--kakoune	Kakoune is a code editor. Prior to version 2026.05.21, the bundled, enabled by default, `autorestore.kak` script can be exploited by malicious backup files leading	2026-08-07	8.6	CVE-2026-48120

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to arbitrary kakoune and shell commands being executed by simply opening a file. Kakoune 2026.05.21 fixes the issue. As a workaround, add `autorestore-disable` to the user kakrc will disable the autorestore feature.			
maximeAmini--Atals-Livre	Atlas-Livre contains an improper access control vulnerability in the admin controllers under Espace_admin/controleur/ that allows unauthenticated attackers to bypass session-based authentication guards by sending raw HTTP requests that ignore redirects. Attackers can invoke destructive admin actions such as record deletion by requesting controller endpoints with GET parameters like supp, because the PHP header() redirect is never followed by an exit or die call, allowing all subsequent code including database operations to execute regardless of session state.	2026-08-04	9.8	CVE-2026-69703
MaxSite--MaxSite CMS	MaxSite CMS 109.5 and earlier contains an authentication bypass vulnerability in the AJAX dispatcher that allows unauthenticated attackers to access admin-gated endpoints by supplying any X-Requested-With header and requesting a base64-encoded path resolving to any *-ajax.php file in the codebase. Attackers can exploit this dispatcher bypass to reach privileged plugin endpoints without credentials, enabling actions such as manipulating poll states and vote counts, and amplifying the impact of any dangerous operation performed by admin-only ajax files across the plugin tree.	2026-08-04	9.8	CVE-2026-70552
MaxSite--MaxSite CMS	MaxSite CMS contains a remote code execution vulnerability that allows unauthenticated attackers to inject arbitrary PHP code into the application configuration file by submitting crafted POST requests to the install endpoint after installation is complete. Attackers can supply a malicious db_dbprefix value containing a single quote to break out of a PHP string literal in application/config/database.php, appending attacker-controlled PHP statements that are executed by the web server on every subsequent request, resulting in persistent unauthenticated remote code execution as the web-server process user.	2026-08-04	9.8	CVE-2026-70553
MaxSite--MaxSite CMS	MaxSite CMS contains a PHP object injection vulnerability that allows unauthenticated attackers to execute arbitrary code by passing attacker-controlled serialized data in the maxsite_comuser cookie directly to unserialize() without validation or class allowlisting. Attackers can craft a malicious serialized PHP object payload delivered in a single HTTP request to trigger magic methods during object graph reconstruction, enabling property-oriented programming attacks or remote code execution via available gadget chains such as those targeting SoapClient or Imagick extensions.	2026-08-04	9.8	CVE-2026-70554
Menulux Software Inc.--Mobile App	Authorization bypass through User-Controlled key vulnerability in Menulux Software Inc. Mobile App allows Software Integrity Attack. This issue affects Mobile App: through 12.05.2026.	2026-08-03	9.8	CVE-2026-2346
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. In versions prior to 4.6.40, the bundled Claude GitHub Actions workflow is vulnerable to command injection because it embeds an attacker-controlled pull request branch name into a Bash run: block without quoting or validation. Additionally, the workflow allows any @claude comment to trigger the job regardless of whether the commenter is a trusted collaborator. An outside contributor can open a pull request from a fork whose branch name contains shell metacharacters and comment @claude, causing Bash to execute arbitrary shell code in the GitHub Actions runner. Because these commands run in a job holding a GitHub App token with write permissions, OIDC access, and gh/git access, the injection can be chained through \$GITHUB_PATH to compromise later privileged steps, enabling repository writes, pull request and issue manipulation, or OIDC-token abuse. This issue has been fixed in version 4.6.40.	2026-08-05	10	CVE-2026-48168
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. In versions 3.9.26 through 4.6.57 of praiseonai and 0.12.12 through 1.6.57 of praiseonaiagents, the workflow "include" feature is vulnerable to code execution. Workflow._execute_include() implicitly imports and runs an included recipe's tools.py via a raw importlib.util.spec_from_file_location() and spec.loader.exec_module() call, without honoring the PRAISONAI_ALLOW_TEMPLATE_TOOLS/PRAISONAI_ALLOW_LOCAL_TOOLS autoload opt-in gates or routing through the centralized safe loader that protects the other tools.py autoload paths. As a result, a workflow that includes an attacker-controlled local recipe directory executes arbitrary module-level Python code during include setup, before any child workflow parsing or model call, and the same sink is reachable through the higher-level praisonai.recipe.run() recipe API. An attacker who can cause a victim process to run a workflow or recipe that	2026-08-05	7.8	CVE-2026-55522

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	includes an untrusted local recipe achieves arbitrary Python code execution as the PraisnAI process user, a variant that bypasses the hardening applied to the previously disclosed automatic tools.py RCE advisory family. This issue has been fixed in version 4.6.58 of praisnai and 1.6.58 of praisnaiagents.			
MervinPraisn-- PraisnAI	PraisnAI is a multi-agent teams system. In versions prior to 1.6.58, the web_crawl tool performs its SSRF check only on the initially supplied URL, allowing the protection to be bypassed so the tool connects to attacker-chosen internal destinations. The check resolves the hostname once with socket.gethostbyname and rejects private/loopback/link-local results, but then passes the URL to a fetcher using httpx.Client(follow_redirects=True) (or urllib.request.urlopen when httpx is absent, which also follows redirects) that re-resolves the hostname at connect time with no further validation. This validate-here/fetch-there gap is exploitable through both HTTP redirects and DNS rebinding. If an attacker can influence URLs passed to web_crawl(), directly or through an agent/tool workflow, they can cause the PraisnAI host to fetch loopback, private-network, or cloud metadata endpoints reachable from that host, with the response body returned in the web_crawl() result. This issue has been fixed in version 1.6.58.	2026-08-05	7.5	CVE-2026-55524
MervinPraisn-- praisnai-platform	PraisnAI is a multi-agent teams system. Versions prior to 0.1.4 of the PraisnAI Platform API have two authorization failures that together break workspace isolation. The service layer for issues and projects performs global primary-key lookups without checking workspace ownership, so any authenticated user can read, modify, and delete resources in any workspace just by swapping UUIDs in their API requests. On top of that, every member management endpoint (add, update role, remove) only requires `min_role="member"`, which lets any workspace member promote themselves to owner and kick out the original owner. A low-privilege member of one workspace can steal data from every other workspace and take over any workspace they belong to. Both issues come from the same gap: the route layer pulls `workspace_id` from the URL and verifies membership, but the service layer ignores the workspace scope for resource lookups and ignores the caller's role level for member operations. The `require_workspace_member()` dependency does its job correctly. The problem is that the service layer doesn't use the information it provides. Version 0.1.4 of the PraisnAI Platform API patch the issue.	2026-08-07	8.8	CVE-2026-48169
Miantang--IoT-PHP	Miantang/IoT-PHP's index.php implements a POST /userlogin route that reads the password directly from \$_POST['pwd'] with no sanitization and concatenates it into a raw SQL string: mysql_query("select * from userlists where username='\$username' and password='\$password' limit 1"). The username value is passed through htmlspecialchars(), which does not encode single quotes by default and therefore does not prevent SQL injection through the password field. An unauthenticated attacker can submit a payload such as pwd=' OR '1'='1 to bypass authentication and, via UNION-based injection, extract arbitrary data from the database.	2026-08-05	9.8	CVE-2026-71237
Microck-- opencode-studio	OpenCode Studio before 2.4.4 contains a missing authentication vulnerability that allows unauthenticated remote attackers to read arbitrary files within the temp and static/music directories by directly accessing the GET /api/tmp/:tmpFile and GET /api/music/:fileName endpoints. Attackers can retrieve intermediate audio, video artifacts, and subtitles belonging to other users' jobs, and additionally delete any video by ID through the unauthenticated DELETE /api/short-video/:videoid endpoint.	2026-08-04	9.1	CVE-2026-69110
Microsoft-- Application Insights Profiler	Improper limitation of a pathname to a restricted directory ('path traversal') in Application Insights Profiler allows an authorized attacker to elevate privileges over a network.	2026-08-06	8.8	CVE-2026-49163
Microsoft--Azure Active Directory	Modification of assumed-immutable data (maid) in Azure Active Directory allows an authorized attacker to elevate privileges over a network.	2026-08-06	9.9	CVE-2026-50481
Microsoft--Azure Confidential Ledger	Exposed dangerous method or function in Azure Confidential Ledger allows an authorized attacker to execute code over a network.	2026-08-06	9.1	CVE-2026-68823
Microsoft--Azure Logic Apps	Improper access control in Azure Logic Apps allows an authorized attacker to disclose information over a network.	2026-08-06	9.6	CVE-2026-56161
Microsoft--Azure Service Bus	Deserialization of untrusted data in Azure Service Bus allows an authorized attacker to execute code over a network.	2026-08-06	9.9	CVE-2026-50515
Microsoft--Azure SQL Database	Improper authentication in Azure SQL Database allows an unauthorized attacker to elevate privileges over a network.	2026-08-06	10	CVE-2026-56162

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Azure SQL Managed Instance	Improper restriction of communication channel to intended endpoints in Azure SQL Managed Instance allows an unauthorized attacker to elevate privileges over a network.	2026-08-06	8.7	CVE-2026-62836
Microsoft--Azure SRE Agent	Missing authorization in Azure SRE Agent allows an authorized attacker to elevate privileges over a network.	2026-08-06	9.9	CVE-2026-62830
Microsoft--Microsoft 365 Admin Center	Improper verification of cryptographic signature in Microsoft 365 Admin Center allows an unauthorized attacker to elevate privileges over a network.	2026-08-06	9.8	CVE-2026-62873
Microsoft--Microsoft 365 Apps for Enterprise	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code over a network.	2026-08-03	8.8	CVE-2026-62870
Microsoft--Microsoft Edge (Chromium-based)	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2026-08-03	8.1	CVE-2026-66318
Microsoft--Microsoft Edge (Chromium-based)	External control of file name or path in Microsoft Edge for Android allows an unauthorized attacker to disclose information over a network.	2026-08-03	7.4	CVE-2026-65802
Microsoft--Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-08-03	7.5	CVE-2026-66315
Microsoft--Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-08-03	7.4	CVE-2026-66321
Microsoft--Microsoft Edge (Chromium-based)	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-08-03	7.1	CVE-2026-66322
Microsoft--Microsoft Edge for Android	External control of file name or path in Microsoft Edge for Android allows an unauthorized attacker to disclose information locally.	2026-08-03	7.7	CVE-2026-66310
Microsoft--Microsoft Entra Provisioning Service	'.../.../' in Microsoft Entra Provisioning Service (SyncFabric) allows an authorized attacker to elevate privileges over a network.	2026-08-06	9.9	CVE-2026-59115
Microsoft--Microsoft Planetary Computer Pro (GeoCatalog)	Missing authentication for critical function in Microsoft Planetary Computer Pro allows an unauthorized attacker to elevate privileges over a network.	2026-08-06	10	CVE-2026-63508
Microsoft--Microsoft Power Apps	Improper authorization in Microsoft Power Apps allows an unauthorized attacker to elevate privileges over a network.	2026-08-06	9.3	CVE-2026-59118
Microsoft--Microsoft Purview eDiscovery	Improper access control in Microsoft Purview eDiscovery allows an authorized attacker to elevate privileges over a network.	2026-08-06	8.8	CVE-2026-65668
Microsoft--Microsoft SharePoint Online	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	2026-08-06	9.6	CVE-2026-70332
Microsoft--Microsoft Teams	Missing authorization in Microsoft Teams allows an unauthorized attacker to elevate privileges over a network.	2026-08-06	10	CVE-2026-65667
Microsoft--Microsoft Teams	Improper authentication in Microsoft Teams allows an authorized attacker to elevate privileges over a network.	2026-08-06	9.6	CVE-2026-62896
Microsoft--Microsoft Teams	Improper verification of cryptographic signature in Microsoft Teams allows an unauthorized attacker to perform spoofing over a network.	2026-08-06	7.5	CVE-2026-62918
MihChe--WPBruiser {no-Captcha anti-Spam}	Unauthenticated PHP Object Injection in WPBruiser {no- Captcha anti-Spam} <= 3.1.43 versions.	2026-08-06	9.8	CVE-2026-65556
milvus-io--milvus	Milvus through 2.6.22 and 3.0.0 contains an unauthenticated denial of service vulnerability that allows remote attackers to terminate service components by sending a crafted HTTP GET request to the management server on port 9091. Attackers can exploit the unprotected /management/stop endpoint, which bypasses REST API authentication middleware, by supplying a 'role' parameter to shut down the proxy, datanode, or querynode components, resulting in denial of service.	2026-08-05	7.5	CVE-2026-69111

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MingSoft--MCMS	A vulnerability was determined in MingSoft MCMS up to 3.0.6. This affects the function ModelDataImpl.queryDiyFormData of the file /mdiy/form/data/list.do of the component ms-mdiy. Executing a manipulation of the argument formFields can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-09	7.3	CVE-2026-19355
miniOrange 2FA--miniOrange 2FA	The miniOrange 2FA WordPress plugin before 6.2.8 does not correctly limit the number of second-factor verification attempts, tracking them against a client-supplied identifier that is reissued on every login, allowing an attacker who already knows a user's password to guess the one-time code without limit and take over the account.	2026-08-06	7.5	CVE-2026-16619
miniOrange--WP OAuth Server	Unauthenticated SQL Injection in WP OAuth Server <= 6.2.0 versions.	2026-08-06	9.3	CVE-2026-65520
mistralai--mistral-vibe	Mistral Vibe before 2.23.3 contains a remote code execution vulnerability that allows attackers to execute arbitrary commands by embedding a malicious core.fsmonitor hook in a repository's .git/config file, which is triggered when vibe invokes git status --porcelain without suppressing hook execution. Attackers can distribute or create a crafted repository containing a malicious fsmonitor entry to achieve arbitrary command execution with the victim's full privileges when any vibe command is run inside that repository.	2026-08-05	8.8	CVE-2026-67623
mlflow--mlflow	MLflow's AI Gateway accepts an auth_config.api_base value when creating a gateway secret (mlflow/server/handlers.py, _create_gateway_secret) with no validation of scheme, host, or IP range; the value is stored verbatim. The gateway proxy endpoint (mlflow/server/gateway_api.py, raw_proxy) subsequently issues an HTTP request to that stored api_base plus a caller-supplied path and returns the full response body. MLflow's existing SSRF guard, _validate_webhook_url (which blocks non-global and metadata IPs), is never invoked anywhere in this gateway secret/proxy code path. The CreateGatewaySecret action additionally has no entry in the permission-validator map, so it requires only basic authentication rather than any specific scope, meaning any authenticated user - including read-only accounts - can create a secret pointing at an internal address and reach it via the proxy endpoint, potentially exposing cloud-instance IAM credentials via metadata services. This is related to CVE-2026-4035, which addresses a distinct mechanism in the same gateway-secret feature (server-side \$ENV_VAR resolution inside the api_key field leaking credentials to the configured upstream); the finding here is an independent missing-validation gap in the api_base destination itself, unaffected by that fix.	2026-08-05	7.1	CVE-2026-71211
MonsterInsights Pro--MonsterInsights Pro	The official MonsterInsights Pro update distribution bucket ('monster-insights.s3.amazonaws.com') was compromised. Both the current release (10.2.2) and the version MonsterInsights rolled back to (10.2.0) contain a malicious file, 'class-system-check.php'. Three distinct variants were observed on 2026-06-11, all sharing the same AES-256-GCM key, confirming a single threat actor. The attacker retains write access to the S3 bucket and has been actively iterating on the payload throughout the day.	2026-08-06	10	CVE-2026-11976
mrswapnilsahu--Stock-Inventory-Management-System	The Stock-Inventory-Management-System application's login.php assigns raw \$_POST username/password values to \$_SESSION and builds its authentication query by directly concatenating those session values into a SQL statement with no parameterization or escaping. An unauthenticated remote attacker can submit a payload such as ' OR '1'='1 in the login form to bypass authentication entirely. The same script additionally contains hardcoded administrative credentials (admin/neola) in a post-login conditional check, providing a second, independent full-authentication-bypass path.	2026-08-05	9.8	CVE-2026-71207
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the wps.cgi interface that allows remote attackers to execute arbitrary commands by injecting malicious input through the pin2g, pin5g, or pin6g parameters. Attackers can exploit these unsanitized parameters to execute arbitrary commands on the affected device and obtain root privileges.	2026-08-08	9.8	CVE-2026-71983
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the urlfilter function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit the urlfilter function to inject malicious commands and obtain root privileges on the underlying system.	2026-08-08	9.8	CVE-2026-71984
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the accesscontrol function that allows remote attackers to	2026-08-08	9.8	CVE-2026-71985

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the accesscontrol function to execute malicious commands and obtain root privileges on the underlying system.			
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the dmz function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the dmz function to execute malicious commands and obtain root privileges on the underlying system.	2026-08-08	9.8	CVE-2026-71986
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the alg function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the alg function to execute malicious commands and obtain root privileges on the underlying system.	2026-08-08	9.8	CVE-2026-71987
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the portFw function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the alg function to execute malicious commands and obtain root privileges on the underlying system.	2026-08-08	9.8	CVE-2026-71988
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the porTrigger function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the alg function to execute malicious commands and obtain root privileges on the underlying system.	2026-08-08	9.8	CVE-2026-71989
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the TelnetSSH function used for SSH configuration that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the SSH configuration interface to inject malicious commands and obtain root privileges on the underlying system.	2026-08-08	9.8	CVE-2026-71990
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the TelnetSSH function used for Telnet configuration that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit this vulnerability through the Telnet configuration interface to inject malicious commands and obtain root privileges on the underlying system.	2026-08-08	9.8	CVE-2026-71991
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the macfilter function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit the macfilter function to inject malicious commands and obtain root privileges on the underlying system.	2026-08-08	9.8	CVE-2026-71992
MSI--Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the openvpn function that allows remote attackers to execute arbitrary commands on the affected device. Attackers can exploit the macfilter function to inject malicious commands and obtain root privileges on the underlying system.	2026-08-09	9.8	CVE-2026-71993
Muffingroup--Betheme	Contributor Remote Code Execution (RCE) in Betheme <= 28.4.2 versions.	2026-08-06	9.9	CVE-2026-65548
nanocoai--NanoClaw	A security vulnerability has been detected in nanocoai NanoClaw up to 2.0.64. This affects an unknown part of the file container/agent-runner/src/mcp-tools/core.ts of the component send_file. Such manipulation leads to path traversal. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	7.3	CVE-2026-18991
NASA-AMMOS--anms	The NASA-AMMOS Asynchronous Network Management System (ANMS) reference implementation's default docker-compose.yml publishes the amp-manager service's REST API directly to the host network interface (port 8089, e.g. "\${ION_MGR_PORT:-8089}:8089/tcp") with cap_add: NET_ADMIN, NET_RAW, SYS_NICE, bypassing the CAM (Configuration and Access Manager) gateway that is otherwise the system's sole authentication boundary. The underlying REST server, implemented with CivetWeb in JHUAPL/dtnma-tools (src/refdm/nm_rest.c), is configured with enable_auth_domain_check set to "no" and registers every route, including the DTNMA agent command-dispatch endpoints (.../agents/{eid idx}/send, which accept and forward EXECSET-encoded command sets to a registered DTNMA agent), with a null authentication callback. Any network-reachable client can therefore enumerate registered agents, submit arbitrary command sets to them, and clear stored reports, entirely without	2026-08-05	9.8	CVE-2026-71289

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	credentials. This affects NASA-AMMOS/anms and JHUAPL-DTNMA/dtnma-tools as published; both repositories present this as a reference/ground DTN network-management implementation and testbed, and the affected components communicate with DTNMA agents (which may represent simulated or real spacecraft/ground nodes depending on deployment) rather than being flight software running onboard a spacecraft.			
NASA-AMMOS--plandev (sequencing-server)	The Aerie/PlanDev sequencing-server's authorization middleware (sequencing-server/src/app.ts) derives the caller's Hasura session role via getHasuraSession(), which prefers a session_variables object taken directly from the client-supplied JSON request body over the Authorization header's JWT claims, with no verification that the request actually originated from Hasura. By setting {"session_variables":{"x-hasura-role":"aerie_admin"}} in the body of a request to POST /command-expansion/put-expansion with no Authorization header, an unauthenticated attacker satisfies the role check and can insert arbitrary expansion rules into sequencing.expansion_rule, which govern how spacecraft activities are translated into commands. Separately, POST /put-dictionary is explicitly listed in the ENDPOINTS_WHITELIST and is exempt from any authentication, allowing unauthenticated writes of command dictionaries.	2026-08-05	9.8	CVE-2026-71214
National Security Agency--Ghidra	Ghidra contains an arbitrary code execution vulnerability in the Swift demangler analyzer that allows an attacker to execute arbitrary binaries by supplying a malicious Ghidra project with a crafted Swift tool directory path. When a victim opens the attacker-supplied project, SwiftDemanglerAnalyzer restores the persisted Swift binary directory from project state and SwiftNativeDemangler executes the resolved binary without integrity or signature verification, causing attacker-controlled executables to run under the Ghidra process user with no prompt or confirmation.	2026-08-03	7	CVE-2026-18718
Nexcess--GiveWP	Unauthenticated Cross Site Scripting (XSS) in GiveWP <= 4.16.5 versions.	2026-08-06	7.1	CVE-2026-66690
Nexcess--Kadence WooCommerce Email Designer	Unauthenticated Privilege Escalation in Kadence WooCommerce Email Designer <= 1.5.19 versions.	2026-08-06	9.8	CVE-2026-28005
NexTor--NexTor IP Changer	NexTor IP Changer is a command-line tool that leverages the Tor network to periodically rotate a user's IP address. Versions prior to 2.0.0 have a command execution vulnerability due to unsafe use of `shell=True` with commands that rely on executable resolution through the `PATH` environment variable. An attacker controlling the execution environment can place malicious executables such as sudo earlier in the `PATH`, resulting in execution of attacker-controlled code. Version 2.0.0 fixes the issue.	2026-08-07	7.8	CVE-2026-48097
NexTor--NexTor IP Changer	NexTor IP Changer is a command-line tool that leverages the Tor network to periodically rotate a user's IP address. Versions prior to 2.0.0 execute privileged system commands using `sudo` and `shell=True` directly inside application logic. In environments where passwordless sudo (`NOPASSWD`) is enabled, privileged commands may execute silently without explicit user confirmation. Version 2.0.0 fixes the issue.	2026-08-07	7.3	CVE-2026-48098
NI--NI-PAL	There is a local privilege escalation vulnerability recently discovered in the NI-PAL kernel driver. This may allow a local, authenticated user to escalate privileges and execute arbitrary code. This vulnerability affects NI-PAL 26.3.1 and prior versions running on Microsoft Windows.	2026-08-05	7.8	CVE-2026-18485
nickboss--WordPress File Upload	Unauthenticated SQL Injection in WordPress File Upload <= 5.1.7 versions.	2026-08-06	9.3	CVE-2026-66447
node-red--node-red	Node-RED's local-filesystem library storage module (getLibraryEntry() and saveLibraryEntry()) in packages/node_modules/@node-red/runtime/lib/storage/localfilesystem/library.js, reachable via GET/POST /library/:lib/:type/*path, joins the user-supplied path parameter directly into the filesystem path via fspath.join(libDir, type, path) with no traversal sanitization, containment check, or path normalization/prefix verification. An authenticated user (including read-only-scoped tokens for the read path) can supply a path containing `../` sequences to read arbitrary files outside the library directory; a user with write access can write arbitrary files, enabling remote code execution via SSH authorized_keys or cron injection. This is a distinct, separately unpatched traversal from the previously fixed CVE-2021-21298 (Projects API).	2026-08-05	7.2	CVE-2026-71269
NSquared--Simply Schedule Appointments	Unauthenticated SQL Injection in Simply Schedule Appointments <= 1.6.12.10 versions.	2026-08-06	9.3	CVE-2026-65508

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NSquared--Simply Schedule Appointments	Unauthenticated Cross Site Scripting (XSS) in Simply Schedule Appointments <= 1.6.12.10 versions.	2026-08-06	7.1	CVE-2026-65513
nuxsmmin--sysPass	sysPass's FileBackupService::doBackupFiles() in lib/SP/Services/Backup/FileBackupService.php around line 388 builds a tar shell command by string-concatenating the backup directory path \$this->path directly into the command line ('tar czf ' . \$backupFileApp . ' ' . BASE_PATH . ' --exclude \'' . \$this->path . '\' 2>&1') and passes the result to PHP's exec() with no application of escapeshellarg() and no validation of the path against a safe character set. The \$this->path value is read from the sysPass configuration, which is persisted in the database and writable through the admin settings API and the admin UI. An administrator (or an attacker who has obtained an admin API token or admin session) can therefore store a backup path containing shell metacharacters and trigger a backup operation to execute arbitrary OS commands as the web server process user (typically www-data or apache). Because sysPass is a password manager whose sole purpose is to hold credentials for other systems, code execution as the web-server user permits reading sysPass's master password and encryption key from memory or configuration files, decrypting every stored credential in the database, exporting the entire password vault, pivoting to internal systems using the disclosed credentials, and installing persistent backdoors on the password-manager host.	2026-08-06	7.2	CVE-2026-63725
nuxt--devtools	Nuxt is an open-source web development framework for Vue.js. Prior to 3.3.1, Nuxt DevTools (development mode only) exposes a bidirectional RPC channel over the Vite HMR WebSocket via the nuxt:devtools:rpc plugin. On affected versions the channel has no authentication: any client that can reach the Vite HMR endpoint (ws://<host>:<port>/, subprotocol vite-hmr) can call RPC methods, with no token, handshake, or origin check before the channel is established. The updateOptions(), clearOptions(), and openInEditor() methods do not enforce the ensureDevAuthToken check that the other mutating methods use. openInEditor() reads the persisted behavior.openInEditor value and passes it to the launch-editor package, which spawns it as a child process. That value is settable through the equally unauthenticated updateOptions(). An attacker who can reach the HMR port can therefore chain updateOptions('behavior', { openInEditor: '<command>' }) then openInEditor('<any-existing-file>') to execute an arbitrary program on the developer's machine. This issue is fixed in 3.3.1.	2026-08-05	9.6	CVE-2026-71319
nuxt--nuxt	Nuxt is an open-source web development framework for Vue.js. From 3.21.7 until 3.21.10 and 4.5.1, mixed-case routeRules keys can fail to match case-folded lookups when router.options.sensitive is false and drop appMiddleware authorization gates. This is caused by an incomplete fix for CVE-2026-53721. This issue is fixed in 3.21.10 and 4.5.1.	2026-08-05	8.2	CVE-2026-71315
nuxt--nuxt	Nuxt is an open-source web development framework for Vue.js. From 3.4.0 until 3.21.10 and 4.5.1, an attacker can inject a template key through /__nuxt_island/ props into a dynamic component when `vue.runtimeCompiler: true` is enabled, causing template execution in the Nitro process. This issue is fixed in 3.21.10 and 4.5.1.	2026-08-05	8.1	CVE-2026-71320
nuxt--nuxt	Nuxt is an open-source web development framework for Vue.js. From 3.1.0 until 3.21.10 and 4.5.1, an unauthenticated attacker can use a server island v-for prop, including vforToArray and , to trigger unbounded SSR memory allocation until MAX_VFOR_LENGTH = 100000 and crash the Nuxt process. This issue is fixed in 3.21.10 and 4.5.1.	2026-08-05	7.5	CVE-2026-71314
nuxt--nuxt	Nuxt is an open-source web development framework for Vue.js. From 4.4.0 until 4.5.1, runtime cache:nuxt:payload entries for /<page>/_payload.json can be returned before route middleware and page guards because import.meta.prerender is not enforced, disclosing another user's SSR data. This issue is fixed in 4.5.1.	2026-08-05	7.5	CVE-2026-71316
nuxt--nuxt	Nuxt is an open-source web development framework for Vue.js. From 3.1.0 until 3.21.10 and 4.5.1, the internal island renderer endpoint '/__nuxt_island/...' decodes and hashes attacker-controlled JSON body input with destr and ohash before validating the URL-resident hash. An unauthenticated `POST /__nuxt_island/_json` with a large JSON body is fully read, parsed, hashed, and then rejected, which wastes CPU on Nitro single event loop and delays concurrent requests. No valid hash and no authentication are required. This issue is fixed in 3.21.10 and 4.5.1.	2026-08-05	7.5	CVE-2026-71321

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability in the multimodal serving topology, where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	2026-08-04	9.8	CVE-2026-24254
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause an out-of-bounds write. A successful exploit of this vulnerability might lead to denial of service and data tampering.	2026-08-04	8.2	CVE-2026-24253
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to denial of service and data tampering.	2026-08-04	8.2	CVE-2026-47623
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability in the multimodal embedding cache, where an attacker could cause a hash collision by submitting images that share an identical pixel byte sequence but have different dimensions. A successful exploit of this vulnerability might lead to data tampering.	2026-08-04	7.5	CVE-2026-24255
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability in the image loading component where an attacker may cause improper limitation of a pathname to a restricted directory. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-04	7.5	CVE-2026-47612
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability where an attacker may cause improper limitation of a pathname to a restricted directory by supplying a crafted local path in a multimodal request. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-04	7.5	CVE-2026-47613
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability where an attacker may cause server-side request forgery. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-04	7.5	CVE-2026-47614
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability where an attacker may cause server-side request forgery by supplying a crafted URL in a multimodal request. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-04	7.5	CVE-2026-47615
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability in the multimodal media fetcher where an attacker may cause server-side request forgery. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-04	7.5	CVE-2026-47616
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability in the multimodal media fetcher where an attacker may cause server-side request forgery via DNS rebinding. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-04	7.5	CVE-2026-47617
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability in the Rust multimodal media fetcher where an attacker could cause server-side request forgery. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-04	7.5	CVE-2026-47618
odysseus-dev--odysseus	Odysseus before commit bf325f6 contains a missing authorization vulnerability that allows authenticated non-admin users to manage server-wide embedding backend configuration by invoking endpoint management routes that verify session authentication but omit the admin authorization guard. Attackers can supply an attacker-controlled URL to overwrite the embedding backend persisted in the endpoint configuration file and process environment, causing all subsequent embedding operations including chat messages, RAG queries, memory entries, and vault text to be transmitted in plaintext to the attacker-controlled destination, or delete the endpoint configuration to deny embedding service to all users.	2026-08-04	8.8	CVE-2026-70619
OMICRON electronics GmbH--OMICRON StationGuard	OMICRON StationGuard before version 4.10 contains a cryptographic timing side-channel vulnerability in the backend authentication mechanism that may allow an unauthenticated attacker to forge valid authentication credentials, bypass authentication and authorization, and impersonate legitimate clients. An attacker can gain full access to the system configuration, allowing modification, reset, or unauthorized alteration of system parameters.	2026-08-06	8.7	CVE-2026-16315
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.1, a fully provisioned OpenReception instance accepts unauthenticated POST requests to `/setup/create-admin-account` and creates additional GLOBAL_ADMIN accounts without verifying that an admin already exists. Any unauthenticated network attacker who can submit a same-origin form POST gains full platform-level administrative control. The newly created account is `is_active=true` with `confirmation_state=ACCESS_GRANTED` and does not require completing email confirmation; the GLOBAL_ADMIN row is created active and immediately usable. Login and tenant enumeration succeed without any further interaction. This is distinct from the deployment race condition already documented on the `Claiming an instance` page. That documented race covers the window between deployment	2026-08-06	9.8	CVE-2026-48085

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and first claim. The bug reported here works after the operator has properly claimed and configured the instance: the layout-level guard that protects the setup page only redirects on GET, while the `default` form action handler creates the user without rechecking `adminExists()`. Three GLOBAL_ADMIN accounts were created in succession during testing, with no rate limiting observed. Audit-specific event logging beyond standard application logs was not assessed; the standard `[error]` line that surfaces only when a uniqueness conflict is hit is not the same as a security event for "additional admin created post-claim". The form post is rejected for browser drive-by CSRF by SvelteKit's built-in same-origin check, but any tool that supplies a matching `Origin` header (curl, Burp, automated scanners, server-side proxies) bypasses this trivially. No additional preconditions exist. Users should upgrade to version 1.0.1 to receive a patch.			
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.2, a TENANT_ADMIN promotes themselves to platform-wide GLOBAL_ADMIN through a single PUT request. The role-update handler accepts the `GLOBAL_ADMIN` enum value from any tenant admin updating their own tenant's staff. No policy check enforces that "only an existing GLOBAL_ADMIN may grant GLOBAL_ADMIN", so the schema validation IS the authorization decision. After re-login, the JWT contains the new role and the formerly-tenant-scoped admin reaches every other tenant on the platform. On the hosted OpenReception service this is a scope-changed escalation: a single customer-side tenant administrator gains full platform-wide administrative control over all other tenants' configuration, users, staff records, operational metadata, and tenant lifecycle. Plaintext appointment contents remain subject to the E2E model unless chained with the staff-crypto poisoning issue (V-4) or with staff-passkey hijacking (V-1). On a single-tenant self-hosted deployment it is still a privilege escalation because TENANT_ADMIN should not be able to create new tenants, modify global configuration, or manage other administrators. The same handler also accepts updates targeted at any colleague within the tenant. A tenant admin can promote a separate collaborator account instead of themselves, leaving their own audit trail clean while the platform-wide breach happens through a separate identity. Version 1.0.2 fixes the issue.	2026-08-06	9.9	CVE-2026-48086
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.2, the registration handler at `POST /api/auth/register/{userId}` validates the relationship between the WebAuthn challenge and the registration cookie's email but never validates that the `userId` in the URL belongs to that email. An unauthenticated attacker requests a challenge for their own email, generates a registration response with their own authenticator, and submits it against any victim user's URL. The challenge-vs-cookie email match passes, the WebAuthn ceremony validates, and `addPasskey` writes the attacker's credential into the victim's `user_passkey` rows. The next victim-email login accepts a passkey assertion from the attacker's authenticator and issues a session as the victim. User IDs are not strictly secret on this platform, but the exact set of exposure surfaces should be assessed by the maintainers. Staff-list endpoints return user IDs to authenticated tenant members per the route signature; live verification of all exposure surfaces (whether user IDs leak through any unauthenticated route, through invite-confirmation URLs, or through other administrative views) is part of the pending live PoC. Where the attacker knows the victim's email and userId, the analysis below becomes account takeover. Version 1.0.2 fixes the issue.	2026-08-06	9.8	CVE-2026-48087
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.4, the route `POST /api/tenants/{tenantId}/staff/{staffId}/crypto` accepts and stores attacker-controlled ML-KEM-768 public keys against any tenant on the platform without authentication. The handler logs an "Unauthorized crypto key storage attempt" warning when neither a session nor a registration cookie is present, then proceeds to insert the row regardless. The platform's E2E claim that "even administrators cannot view sensitive information" is broken: any unauthenticated network attacker can register themselves as an additional encryption recipient for any tenant's future patient appointments. A second variant of the bug suppresses the unauthorized-warning log entry. The Zod schema makes the `email` field optional. When the request body omits `email` and the request carries no registration cookie, the comparison `registrationEmail === email` becomes `undefined === undefined`, which evaluates to `true`. The handler treats the request as a legitimate registration flow, skips the warning entirely, and stores the row.	2026-08-06	9.4	CVE-2026-48088

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Successful storage is still recorded as an `[info]` log line, but the security-relevant warning that operators are most likely to monitor or alert on is gone. The `staff_crypto` table has no unique constraint on `user_id`, so an arbitrary number of attacker rows can coexist for the same staff identifier and all return as `is_active=true`. The supplied `staffid` does not need to match any existing user or pending invite. Schema validation on `passkeyid`, `publicKey`, and `privateKeyShare` is also weak: the literal string ` <placeholder-base64>` was accepted, indicating no length, format, or cryptographic-validity check beyond field presence. This weakness is independent of the auth bypass but compounds it: a poisoned directory can also be filled with malformed entries that break legitimate booking flows. The injected key is consumed by the public booking flow. After completing the unauthenticated `bootstrap-challenge` and `bootstrap-verify` ceremony as a "patient", the resulting `bookingAccessToken` is accepted by `GET /api/tenants/{id}/appointments/staff-public-keys`, which returns the attacker-controlled keys alongside any legitimate ones. A new appointment encrypts its tunnel key with ML-KEM to all listed recipients, so the attacker becomes a co-recipient of the encryption and can decapsulate the tunnel key with the matching secret. From there, all appointment payloads for that booking are decryptable. Version 1.0.4 patches the issue.</placeholder-base64>			
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.2, the `GET /api/tenants/{id}` endpoint returns the full tenant record to any authenticated `TENANT_ADMIN` of that tenant, including the `databaseUrl` field. This field contains the live PostgreSQL connection string the application uses to connect to that tenant's database. In the tested official `docker-compose.prod.yml` deployment, the connection string contained the user `postgres` with `rolsuper=true` and the plaintext password from `secrets/postgres_password.txt`. Operators who configure a non-superuser PostgreSQL user via `secrets/postgres_user.txt` would expose a less privileged credential, but the disclosure of the connection string itself is independent of that choice. The same credential applies to every database managed by that PostgreSQL instance: the central `appointment_booking` database, every per-tenant database (one per tenant), and the postgres administrative database. A `TENANT_ADMIN` of one tenant who can reach `postgres:5432` (directly via internal network, indirectly via any SSRF, RCE, or file-read in the application) can read every other tenant's appointment ciphertexts, key shares, and metadata; read the central user table, including all `GLOBAL_ADMIN` accounts, password hashes, and session records; modify or delete any data in any tenant database; and/or i a superuser-scoped deployment: use PostgreSQL's `pg_read_server_files`, `COPY ... FROM PROGRAM`, and `CREATE EXTENSION` for further escalation inside the database container. This breaks the per-tenant database isolation that is otherwise the primary cross-tenant control in the application. The application code carefully scopes most queries to the calling tenant's database, but those scopings are irrelevant once the attacker holds the credentials that bypass the application entirely. Version 1.0.2 fixes the issue.	2026-08-06	8	CVE-2026-48080
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.2, a `TENANT_ADMIN` can store `javascript:` URLs in the tenant `links` configuration (`website`, `imprint`, `privacyStatement`). These values are returned to the patient-facing landing page via `/api/public`, hydrated into the SvelteKit Button component, and rendered as ` <a href="javascript:...">` elements without URL-scheme filtering. A patient who clicks any such link executes the attacker's JavaScript inside the patient browser origin, where patient form data is read before client-side encryption is applied. This breaks the project's central trust claim that the server is an untrusted relay and that administrators cannot read patient data. Patient-side encryption happens after form input, so JavaScript executing in the patient origin can read or alter the plaintext before encryption is performed. Version 1.0.2 fixes the issue.	2026-08-06	8.1	CVE-2026-48081
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.2, when a user navigates to the `/logout` page, the page's server-side load handler deletes the `access_token` cookie before calling `/api/auth/logout` via an internal `event.fetch()`. The internal fetch consequently runs without the auth cookie, so `apiAuthHandle` rejects it, the logout handler never executes, and `SessionService.revokeSession()` is never called for the current session. The DB session row remains valid until its natural expiry (one week by default). The user sees a successful logout (cookie gone, UI returns to login), but any party still holding a copy of the now-deleted access token can	2026-08-06	7.4	CVE-2026-48079

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	continue making authenticated API calls until the session naturally expires. The root cause is a simple ordering mistake. The same auth subsystem implements the correct order in `/api/auth/logout`: revoke the current DB session first, then delete the cookie. The page-level wrapper does the opposite. Version 1.0.2 initiates server-side logout before removing authentication cookies and first appears in version 1.0.2. Version 2.0.0 later replaces this with a race-free client-side logout flow.			
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Versions prior to 1.0.2 don't throttle failed passphrase login attempts. An attacker can submit unlimited wrong passphrase guesses against any known email address, capped only by the Argon2 verification cost (about 100 milliseconds per attempt on the tested host, giving 10 attempts per second sustained). The same backend implements a working per-account throttle on the WebAuthn challenge endpoint, which returns HTTP 429 after roughly 19 attempts. The passphrase branch simply does not invoke that throttle, leaving a supported high-value login path unprotected against credential stuffing and dictionary attacks. The asymmetry confirms this is an oversight rather than a design choice. The throttle infrastructure exists, is wired into the same auth backend, and works on the WebAuthn path. The passphrase branch in `/api/auth/login` was not updated to record failed attempts. Combined with the application's minimum-passphrase policy (12 characters, no entropy or dictionary checks), accounts using common base patterns such as `Spring2026!XX` or words from a leak corpus are realistically reachable in days on a single CPU, hours on a small GPU farm. Version 1.0.2 patches the issue.	2026-08-06	7.4	CVE-2026-48084
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.0 until 0.11.0, when ENABLE_OAUTH_TOKEN_EXCHANGE=True, /oauth/{provider}/token/exchange accepts a raw provider access token and validates it by calling the provider userinfo endpoint without confirming which OAuth client the token was issued to. Anyone holding an access token minted for any client registered with the same provider could exchange it for an Open WebUI session as that token user, including applications the operator does not control and has never authorized. This issue is fixed in 0.11.0.	2026-08-04	8.1	CVE-2026-70482
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 until 0.11.0, the terminal file-preview serveUrl iframe branch always granted allow-same-origin together with allow-scripts for HTML files served from the application origin. Any authenticated user with access to a configured terminal server could cause script in a previewed file to run in the Open WebUI origin, read the victim's session token from localStorage, and take over the account, with possible server-side code execution if the victim was an admin or held workspace.functions. This issue is fixed in 0.11.0.	2026-08-04	8.2	CVE-2026-70486
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.10.0 until 0.11.0, src/lib/components/chat/Messages/Markdown/KatexRenderer.svelte could store and render a chat message whose math block makes KaTeX fail with a stack overflow instead of a parse error. The catch branch fell back to inserting the original math source into the page as HTML through {@html} rather than as text, so script in the message runs in the browser of whoever views it, including shared chats and channels. The viewer's session token in localStorage can be stolen, and an administrator viewer can have their account taken over. This issue is fixed in 0.11.0.	2026-08-04	8.7	CVE-2026-70492
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.10.0 until 0.11.0, the DELETE /api/v1/folders/{id} handler in backend/open_webui/routers/folders.py allowed a user granted write access to a shared chat folder to permanently delete chats and messages belonging to the folder owner. The cascade following the authorization check is bound to the folder owner's id, but the subfolder check accepted any inherited write grant instead of requiring ownership or administrator status. A collaborator can destroy the owner's subtree or force-move chats out of it when delete_contents=false. This issue is fixed in 0.11.0.	2026-08-04	8.1	CVE-2026-70494
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 until 0.11.0, with WEB_LOADER_ENGINE=playwright, the Playwright web loader validates only the top-level page request and lets sub-resource requests pass unvalidated. A page supplied by an authenticated user can use JavaScript to reach blocked internal addresses, and returned DOM can include	2026-08-04	7.7	CVE-2026-70479

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	data read from those addresses in web-search or RAG output. This issue is fixed in 0.11.0.			
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 until 0.11.0, Open WebUI checked whether a user-supplied URL destination was globally routable by applying <code>ipaddress.is_global</code> to the literal IPv6 address without examining IPv4 addresses embedded in transition encodings. On a deployment with a NAT64 gateway, any verified user could wrap an internal or cloud-metadata IPv4 address in the NAT64 well-known prefix, pass the filter, and receive the internal response body through RAG URL ingestion, URL-to-markdown conversion, or web-search content retrieval. This issue is fixed in 0.11.0.	2026-08-04	7.1	CVE-2026-70485
open62541--open62541 v1.5.5	open62541 1.5.5 contains an out-of-bounds read in the client-side function <code>responseReadNamespacesArray()</code> in <code>src/client/ua_client_connect.c</code> .	2026-08-04	7.5	CVE-2026-67857
open62541--open62541 v1.5.5	Buffer Overflow vulnerability exists in open62541 1.5.5 when the Local Discovery Server (LDS) is built with multicast discovery enabled through the MDNSD backend. An unauthenticated remote attacker can send a RegisterServer or RegisterServer2 request containing many unique discoveryUrls. This allows remote attackers to cause a denial of service.	2026-08-04	7.5	CVE-2026-67858
open62541--open62541 v1.5.5	Buffer Overflow vulnerability in open62541 v1.5.5 allows a remote attacker to cause a denial of service via the Discovery/LDS handling.	2026-08-04	7.5	CVE-2026-67859
open62541--open62541 v1.5.5	An issue in open62541 v1.5.5 and before allows a remote attacker to cause a denial of service via the <code>UA_Client_getRemoteDataTypes</code> component	2026-08-04	7.5	CVE-2026-67861
open62541--open62541 v1.5.5	In open62541 1.5.5, a server-side use-after-free exists in the local MonitoredItem callback path. The issue occurs when <code>UA_Subscription_localPublish</code> continues to use the current <code>UA_Notification</code> after a callback invokes <code>UA_Server_deleteMonitoredItem</code> for the current local MonitoredItem. This allows a remote attacker to cause a denial of service.	2026-08-05	7.5	CVE-2026-67863
open62541--open62541 v1.5.5	Buffer Overflow vulnerability in open62541 v1.5.5 allows a remote attacker to cause a denial of service via the <code>Service_Call</code> validates input arguments against runtime-resolved <code>InputArguments</code> metadata	2026-08-05	7.5	CVE-2026-67869
openemr--openemr	OpenEMR through 8.2.0 contains a remote code execution vulnerability in the document category tree component (<code>library/classes/Tree.class.php</code>) that allows authenticated administrators to execute arbitrary operating system commands by injecting PHP payloads into the categories database table. Attackers can chain arbitrary SQL execution to alter the <code>id</code> column type to <code>VARCHAR</code> and insert a malicious PHP payload, which is then executed via an unsanitized <code>eval()</code> call whenever any page instantiates <code>CategoryTree</code> , including unauthenticated and low-privilege pages, resulting in command execution as the web server user.	2026-08-03	9.1	CVE-2026-39932
openemr--openemr	OpenEMR through 8.2.0 contains an improper authentication vulnerability in the OAuth2 dynamic client registration endpoint that allows unauthenticated attackers to register a malicious client with system-level FHIR scopes by supplying a self-generated RSA keypair via the <code>jwtks</code> field. Once an administrator approves the registered client, attackers can use the <code>client_credentials</code> grant with a self-signed JWT assertion to obtain access tokens granting read access to all FHIR resources across all patients in the system.	2026-08-03	8.1	CVE-2026-67610
openemr--openemr	OpenEMR through 8.2.0 contains an authentication bypass vulnerability that allows attackers with valid credentials to circumvent multi-factor authentication by exploiting the exposed OAuth2 password grant flow through an unauthenticated client registration endpoint. Attackers can register an OAuth2 client via the unauthenticated registration endpoint and use the password grant to exchange credentials for an API access token, bypassing the normal web interface authentication and any enforced multi-factor authentication controls.	2026-08-03	8.1	CVE-2026-67611
openemr--openemr	OpenEMR through 8.2.0 contains an authenticated SQL injection vulnerability in the backup configuration import feature that allows administrators with admin or super ACL privileges to execute arbitrary DDL and DML statements against the application database by uploading a crafted SQL file at the <code>form_step=202</code> parameter in <code>backup.php</code> . Attackers can exploit the unfiltered <code>shell_exec</code> invocation of the <code>mysql</code> command-line client to extract credential hashes, modify access control tables, inject backdoor accounts, create persistent triggers or stored procedures, and write arbitrary files to the filesystem where MySQL FILE privileges and permissive <code>secure_file_priv</code> settings are configured.	2026-08-03	7.2	CVE-2026-39931
openshwprojects--OpenBK7231T_Ap p	OpenBK7231T's <code>CHANNEL_SetLabel()</code> (<code>src/cmds/cmd_channels.c</code>) stores channel labels received via the MQTT <code>SetChannelLabel</code> command using <code>strdup()</code> with no HTML sanitization. <code>CHANNEL_GetLabel()</code> returns these labels unsanitized, and they are rendered via <code>hprintf255()</code> at 15+ locations in <code>src/httpserver/http_fns.c</code> with no	2026-08-05	8.5	CVE-2026-71274

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTML encoding. An attacker with MQTT broker access (commonly unauthenticated in real deployments) can set a channel label containing a <script> payload that executes when any user views the device's web panel.			
OpenSIPS--opensips	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. Versions 3.4.0-beta through 3.6.5 and 4.0.0-beta contain a buffer overflow in the {s.b64encode} string transformation. The size check for {s.b64encode} only verifies that the input fits within the 64 KB transformation buffer, but base64 encoding expands the data by roughly a third, so an input between about 49,153 and 65,535 bytes produces more output than the buffer can hold and overflows it by up to 21,844 bytes. Because these transformation buffers sit next to each other in memory and are reused for chained transformations, the overflow writes attacker-controlled data into the adjacent buffer and corrupts values used by later transformations processing the same SIP message. A remote attacker can trigger this by sending a SIP message with a large header value (roughly 50,000 bytes or more) when the routing script applies {s.b64encode} to attacker-controlled input, making exploitability dependent on the deployment's routing configuration. This issue has been fixed in versions 3.6.6 and 4.0.0-rc1.	2026-08-04	9.1	CVE-2026-45100
OpenSIPS--opensips	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. In versions prior to 3.6.6 and 4.0.0-rc1, the construct_uri() function concatenates multiple URI components (protocol, username, domain, port, params) into a fixed 1024-byte global BSS buffer without any bounds checking. When a routing script calls construct_uri() with an attacker-controlled username, a combined component length exceeding 1024 bytes overflows the buffer, corrupting adjacent global data with attacker-controlled content. The overflow reaches disable_503_translation, a global flag controlling SIP 503 response handling, allowing an attacker to deterministically set the flag via the URI username and alter the server's routing behavior for subsequent messages. Because the same buffer is shared with contact_builder(), the overflow also corrupts that function's data, and without a memory sanitizer the adjacent globals are silently overwritten on every request containing a long username. This issue has been fixed in versions 3.6.6 and 4.0.0-rc1.	2026-08-04	9.1	CVE-2026-45537
OpenSIPS--opensips	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. In versions 4.0.0 and prior, processing a SIP message with a header name longer than 255 bytes causes a stack buffer overflow when sip_to_json() is called in the routing script. Function sip_to_json() (modules/sipmsgops/sipmsgops.c) copies SIP header names into a fixed 255-byte stack buffer without bounds checking, performing a memcpy of the full header-name length even though the SIP parser imposes no such limit (a header name can be roughly 65000 bytes). As a result, when a routing script calls sip_to_json(), a SIP message with a header name longer than 255 bytes triggers a stack buffer overflow in which both the length and content of the overwrite are attacker-controlled, corrupting the saved frame pointer and return address. A single unauthenticated UDP packet to the SIP port (5060) can crash the process or, on builds without stack protections, hijack the return address to achieve remote code execution. This affects deployments whose routing script invokes sip_to_json(). This issue was not fixed at the time of publication.	2026-08-04	9.8	CVE-2026-45538
OpenSIPS--opensips	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. In versions prior to 3.6.6 and 4.0.0-rc1, the TCP message framing layer parses the Content-Length header using unsigned int arithmetic with no overflow check. When an attacker sends a Content-Length value that overflows unsigned int (e.g., 4294967296), the framing layer computes a wrapped-around value (e.g., 0) and splits the TCP stream at the wrong boundary, causing the body of the first SIP message to be processed as a separate message and enabling SIP message smuggling. Because Content-Length is parsed in the transport layer before authentication, an unauthenticated, network-based attacker can smuggle arbitrary SIP messages over any TCP-based transport (proto_tcp, proto_tls, proto_ws, proto_wss) on any instance with TCP enabled, with no routing-script preconditions. This allows smuggled messages to bypass front-end SBC/proxy security policies, inherit the connection's authentication context, and evade rate limiting. This issue has been fixed in versions 3.6.6 and 4.0.0-rc1.	2026-08-04	7.5	CVE-2026-45103
openwrt--luci	OpenWrt luci-app-dockerman (LuCI master and openwrt-25.12 snapshots containing the ucode docker_rpc.uc RPC backend after the JS/ucode conversion) contains an OS command injection vulnerability. The package's read ACL grants broad ubus access to docker.* / docker.container.*, which exposes the docker.container.ttyd_start method even though it performs mutating operations. The run_ttyd handler builds a shell command from the request-controlled id, cmd,	2026-08-03	8.8	CVE-2026-69096

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and uid fields and passes it to system() without quoting or argv-style execution in the rpcd root context. An authenticated attacker holding only the luci-app-dockerman read ACL can inject shell metacharacters (e.g., in id) to execute arbitrary commands as root via an HTTP POST to /ubus. openwrt-24.10 and openwrt-23.05 do not contain this backend and are not affected; no patched version was known as of the advisory.			
openwrt--luci	OpenWrt luci-app-bmx7 before commit 5890760a454dad2cb00389dba2cdc5e779e0ffdd contains a path traversal vulnerability in the bmx7-info CGI script that allows unauthenticated attackers to read files outside the configured runtimeDir. Attackers can supply directory traversal sequences in the query string to escape the intended directory and read sensitive files accessible to the CGI process.	2026-08-03	7.5	CVE-2026-69095
openyak--openyak	OpenYak is a local-first agent runtime for reliable tool-using models, with a desktop workspace built on top. Prior to version 1.1.3, the OpenYak desktop backend binds an HTTP API to `127.0.0.1:<random port>` (commonly 19141) without server-side Origin validation, loopback authentication, or Content-Type enforcement, and with a wildcard CORS policy. Any webpage a user visits while OpenYak is running can issue cross-origin requests to this local server - the browser acts as a proxy into loopback, bypassing OS-level network isolation. Chained, this lets a malicious page execute arbitrary shell commands on the host (RCE) via the build agent with `permission_presets.bash=true`, shut down the service, and exfiltrate chat history and account PII - with no user interaction beyond opening the page. Version 1.1.3 patches the issue.	2026-08-07	9.6	CVE-2026-46409
OpenZeppelin--contracts-wizard	OpenZeppelin Contracts Wizard is a web application to interactively build a contract out of components from OpenZeppelin Contracts. Versions prior to 0.10.9 generate a Hardhat test file (`test/test.ts`) by interpolating user-supplied `opts.name` (ERC20/ERC721) and `opts.uri` (ERC1155) directly into TypeScript string literals at `zip-hardhat.ts:48` and `:50` without any JavaScript string escaping. No authentication is required: an attacker crafts a URL such as `https://wizard[.]openzeppelin[.]com/#/erc20?name=");require("child_process").execSync("...");(" and shares it with a developer. When the victim downloads the resulting zip archive and runs `npx hardhat test`, the injected Node.js code executes with the developer's local OS privileges. Version 0.10.9 fixes the issue.	2026-08-06	8.8	CVE-2026-48054
Passionate Programmer Peter--WP Data Access	Unauthenticated Cross Site Scripting (XSS) in WP Data Access <= 5.5.79 versions.	2026-08-06	7.1	CVE-2026-66663
Payment Gateway for Redsys & WooCommerce Lite--Payment Gateway for Redsys & WooCommerce Lite	The Payment Gateway for Redsys & WooCommerce Lite WordPress plugin before 7.0.2 does not verify the authenticity of incoming payment-provider notifications for one of its payment methods before marking orders as paid, allowing unauthenticated attackers to forge a payment-confirmation callback and complete their own orders without paying.	2026-08-06	7.5	CVE-2026-12584
Payment Plugins for PayPal WooCommerce--Payment Plugins for PayPal WooCommerce	The Payment Plugins for PayPal WooCommerce WordPress plugin before 2.0.20 does not have proper authorization checks on a REST endpoint, allowing unauthenticated users to bypass payments	2026-08-06	7.5	CVE-2026-13399
perspective-dev--perspective	Perspective 5.0.0 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary operating system commands by submitting crafted expression strings to the PolarsVirtualServer backend, which passes client-supplied input directly to Python's eval() with only __builtins__={} cleared. Attackers can exploit Python object attribute traversal through the interpreter's loaded class list to reach subprocess.Popen via a TableValidateExprReq or TableMakeViewReq protobuf message, achieving arbitrary command execution in the Perspective host process.	2026-08-04	8.8	CVE-2026-67195
perspective-dev--perspective	Perspective 5.0.0 contains a denial-of-service vulnerability in the VirtualServer protocol dispatcher that allows unauthenticated remote attackers to crash the server process by sending malformed or incomplete protobuf messages. Attackers can send well-formed requests such as ViewToArrowReq with no viewport set or MakeTableReq with no data field to trigger unwrap() calls on None values at nine distinct sites, causing the process to abort with SIGABRT.	2026-08-04	7.5	CVE-2026-67198

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
perspective-dev--perspective	Perspective 5.0.0 contains a path traversal vulnerability that allows unauthenticated remote attackers to read arbitrary files from the server filesystem by including literal ../ segments in HTTP request URL paths. Attackers can bypass the insufficient query-string-stripping sanitization to traverse outside the configured asset root directory and retrieve sensitive files such as system credentials and application secrets, with results exposed cross-origin due to a wildcard Access-Control-Allow-Origin header set on all responses.	2026-08-04	7.5	CVE-2026-67200
pipeboard-co--meta-ads-mcp	Meta Ads MCP is a Model Context Protocol (MCP) server that lets AI assistants run Meta Ads. Prior to version 1.0.109, `AuthInjectionMiddleware.dispatch()` at `http_auth_integration.py:272` unconditionally forwards unauthenticated Streamable HTTP requests to downstream MCP tool handlers without issuing a `401` response, allowing any network-reachable caller to invoke MCP tools without authentication. When no per-request credential is present, tool handlers fall back to the `META_ACCESS_TOKEN` environment variable, and when the downstream Meta Graph API call fails, `api.py:263-269` serialises the raw `httpx` request URL-including the operator's `access_token` as a query parameter-into the JSON-RPC response body, delivering the credential to the unauthenticated caller. Version 1.0.109 fixes the issue.	2026-08-07	9.1	CVE-2026-48039
pluck-cms--Pluck CMS	Pluck CMS's admin panel relies solely on a Referer-header comparison (requestedByTheSameDomain() in data/inc/functions.admin.php, gating every admin.php action) for CSRF protection, with no per-request anti-CSRF token anywhere in the admin area. When a request carries no Referer/Host information, the function's elseif branch returns true, treating the request as same-origin. Because a cross-site attacker page can suppress the Referer header (e.g. via <meta name=referrer content=no-referrer>), it can force an authenticated administrator's browser to submit forged admin actions with no valid Referer, including creating pages with raw HTML (stored XSS via the rendered page) and installing PHP modules/themes (remote code execution).	2026-08-05	9.6	CVE-2026-70376
pluck-cms--Pluck CMS	Pluck CMS through 4.7.21 restricts dangerous file uploads in its admin file-management feature using a fixed blacklist in data/inc/files.php ('.php','php3','php4','php5','php6','php7','phtml','phtm','pht','.ph3','.ph4','.ph5','.asp','.cgi','.phar'), checked against the last 4-5 characters of the filename. The blacklist omits the '.php8' extension. An authenticated administrator can upload a file named e.g. shell.php8, which is stored unmodified and, on servers running PHP 8.x, is executed as PHP by the web server, resulting in remote code execution.	2026-08-05	7.2	CVE-2026-54416
Power Software--PowerISO	A security flaw has been discovered in Power Software PowerISO 9.3.0.0. Affected by this issue is some unknown functionality in the library C:\Windows\System32\drivers\scdemu.sys of the component Kernel Driver. The manipulation results in improper privilege management. The attack is only possible with local access. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-07	7.8	CVE-2026-19189
Premium SEO--Premium SEO	The Premium SEO WordPress plugin is malicious: it ships an unauthenticated backdoor that creates a hidden administrator account and, in some builds, also enables remote code execution, server-side request forgery and arbitrary front-end script/content injection, giving an unauthenticated attacker full control of the affected site.	2026-08-06	10	CVE-2026-14812
Progress Software Corporation--MarkLogic Server	An improper privilege management vulnerability in the SQL, SPARQL, and Optic REST query interfaces of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an authenticated user with a low-privileged REST role to escalate privileges to administrator. This enables execution of privileged operations and unauthorized data access.	2026-08-05	9.9	CVE-2026-7329
Progress Software Corporation--MarkLogic Server	An improper verification of cryptographic signature vulnerability in the SAML authentication module of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an unauthenticated remote attacker to bypass authentication and impersonate any user, including administrators. This vulnerability affects deployments with SAML single sign-on enabled.	2026-08-05	9.1	CVE-2026-7557
Progress Software Corporation--MarkLogic Server	An improper privilege management vulnerability in the REST API document patch operation of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an authenticated user with a low-privileged REST role to escalate privileges and execute privileged operations against the Security database.	2026-08-05	9.9	CVE-2026-8709
Progress Software Corporation--MarkLogic Server	An HTTP request smuggling vulnerability in the HTTP App Server of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows a remote attacker to bypass authentication and authorization checks, hijack a legitimate user's session, or	2026-08-05	9.1	CVE-2026-9190

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	capture credentials. The vulnerability occurs when a crafted HTTP request containing both Content-Length and Transfer-Encoding headers causes a reverse proxy and MarkLogic Server to interpret request boundaries differently.			
Progress Software Corporation--MarkLogic Server	An authentication bypass vulnerability in the ODBC App Server of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an unauthenticated remote attacker to bypass password verification and execute queries with the privileges of any named user known to the server, including administrators.	2026-08-05	9.8	CVE-2026-9192
Progress Software Corporation--MarkLogic Server	An improper privilege management vulnerability in the Hadoop integration of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an authenticated user with a low-privileged Hadoop role to escalate privileges and execute privileged operations against the Security database.	2026-08-05	9.9	CVE-2026-9193
Progress Software Corporation--MarkLogic Server	A cross-site scripting vulnerability in the Query Console of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows a remote attacker who lures an authenticated administrator to a crafted URL to execute arbitrary JavaScript in the administrator's browser session, capture credentials, and perform privileged actions on the administrator's behalf.	2026-08-05	9.3	CVE-2026-9195
Progress Software Corporation--MarkLogic Server	An improper privilege management vulnerability in the REST API document processing pipeline of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an authenticated user with an administrative REST role to escalate privileges. This can result in unauthorized disclosure of sensitive server-side data when it is accessed by a higher-privileged user.	2026-08-05	8.1	CVE-2026-7327
Progress Software Corporation--MarkLogic Server	A server-side request forgery vulnerability in Progress MarkLogic Server before 11.3.6 and 12.0.3 allows an authenticated user with low-privileged roles to bypass protections for cloud instance metadata endpoints. Successful exploitation can disclose cloud credentials and compromise cloud resources accessible to the host instance.	2026-08-05	8.5	CVE-2026-9203
Progress Software Corporation--MarkLogic Server	A cross-site request forgery vulnerability in the Admin UI of Progress MarkLogic Server before 11.3.6 and 12.0.3 allows a remote attacker who lures an authenticated administrator to a malicious web page to perform administrative actions on the administrator's behalf. This can result in unauthorized changes to security configuration.	2026-08-05	7.5	CVE-2026-7326
Property Hive--Houzez Property Feed	Unauthenticated Cross Site Scripting (XSS) in Houzez Property Feed <= 2.5.48 versions.	2026-08-06	7.1	CVE-2026-65560
Puwell Technology Inc.--IP Camera	Puwell IP Camera firmware versions 2.x through 4.x contains an authentication bypass vulnerability that allows unauthenticated attackers to access device functions by sending protocol-conforming packets over TCP port 23456 without credentials. Attackers can exploit the unvalidated Session field in the proprietary control protocol header to access live video streams, control pan and tilt motors, activate audio functions, and remotely restart the device.	2026-08-04	9.8	CVE-2026-61514
Puwell Technology Inc.--IP Camera	Puwell IP Camera firmware versions 2.x through 4.x contains an unauthenticated command injection vulnerability that allows remote attackers to execute arbitrary operating system commands by sending a crafted JSON payload to the DebugShell interface exposed on TCP port 34567. Attackers can exploit the lack of authentication and input sanitization in the binary protocol service to pass arbitrary commands directly to the underlying operating system, achieving root-level code execution and complete device compromise.	2026-08-04	9.8	CVE-2026-61515
QCODE--Qode Tours	Unauthenticated SQL Injection in Qode Tours <= 3.1.3.1 versions.	2026-08-06	9.3	CVE-2026-65546
qstudio--Export User Data	Subscriber PHP Object Injection in Export User Data <= 2.2.6 versions.	2026-08-06	9.8	CVE-2026-65552
Qualcomm, Inc.--Snapdragon	Memory Corruption when processing Device Capability Extended attributes in certain NAN Service Discovery Frames with invalid length values.	2026-08-04	9.6	CVE-2026-25289
Qualcomm, Inc.--Snapdragon	Cryptographic Issue while processing registration requests with malformed or missing authentication parameters.	2026-08-04	8.1	CVE-2026-24079
Qualcomm, Inc.--Snapdragon	Memory corruption while processing a packet with a size close to the maximum allowed value.	2026-08-04	7.8	CVE-2026-21366
Qualcomm, Inc.--Snapdragon	Memory Corruption when handling malformed request parameters in the fingerprint TA.	2026-08-04	7.8	CVE-2026-24080
Qualcomm, Inc.--Snapdragon	Memory Corruption while processing IOCTL device driver requests with invalid arguments.	2026-08-04	7.8	CVE-2026-24083
Qualcomm, Inc.--Snapdragon	Weak configuration when UE does not verify the consistency of its additional security capabilities with the replayed capabilities.	2026-08-04	7.5	CVE-2026-24084
Qualcomm, Inc.--Snapdragon	Transient DOS when processing a short target wake time channel usage response frame with insufficient packet size.	2026-08-04	7.4	CVE-2026-25288

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Qualcomm, Inc.-- Snapdragon	Memory Corruption when processing untrusted user input in the fastboot command handler for audio framework configuration.	2026-08-04	7.6	CVE-2026-25292
raghav993--toner-management	toner-management's admin state-changing handlers (add.php, edit.php, delete.php under admin/toners, admin/toner-brands, admin/printers, and related admin subdirectories) executed INSERT/UPDATE/DELETE database operations with no authentication or authorization check, while access control was enforced only in listing views. An unauthenticated remote attacker could invoke these handlers directly to create, modify, or destroy application data. The vendor has since merged a fix requiring an authenticated admin session before any such handler proceeds.	2026-08-05	8.2	CVE-2026-71252
Rajat Varlani-- Super Socializer	Unauthenticated Broken Authentication in Super Socializer <= 7.14.5 versions.	2026-08-06	8.8	CVE-2026-65542
Rajat Varlani-- Super Socializer	Unauthenticated Cross Site Scripting (XSS) in Super Socializer <= 7.14.5 versions.	2026-08-06	7.1	CVE-2026-65544
rancher--rancher	Rancher issues long-lived registration tokens to authenticate nodes and agents joining a downstream cluster. These tokens were stored and exposed in plaintext with no expiration, so a malicious user could obtain one either through the Rancher API, etcd, stored automation, or direct file access on a node, and could use it at any time to register a rogue node into the cluster.	2026-08-05	8.8	CVE-2026-55997
Rank Math SEO-- Rank Math SEO	Unauthenticated Cross Site Scripting (XSS) in Rank Math SEO <= 1.0.274.1 versions.	2026-08-06	7.1	CVE-2026-66702
Razer-- RzUpdateService	A weakness has been identified in Razer RzUpdateService 1.10.14.0. Affected by this vulnerability is an unknown functionality of the file C:\Program Files (x86)\Razer\RzUpdateEngineService\RzUpdateService.exe of the component Named Pipe Handler. Executing a manipulation of the argument lpThreadParameter can lead to improper privilege management. The attack requires local access. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure.	2026-08-03	7.8	CVE-2026-18606
rclone--rclone	rclone is a command-line program to sync files and directories to and from different cloud storage providers. Prior to v1.75.0, rclone interpolates remote SFTP paths into PowerShell hash commands in backend/sftp/sftp.go, and quoteOrEscapeShellPath escapes only ASCII apostrophe even though PowerShell treats U+2018, U+2019, U+201A, and U+201B as single-quote delimiters, allowing an attacker-controlled filename to terminate the intended path literal and append PowerShell statements that execute as the victim SSH account when server-side hashing is invoked. This issue is fixed in v1.75.0.	2026-08-05	8	CVE-2026-71312
realmag777-- TableOn WordPress Posts Table Filterable	The TableOn - WordPress Posts Table Filterable plugin for WordPress is vulnerable to blind SQL Injection via the `filter_data[comment_count]` parameter of the public `tableon_get_table_data` AJAX action in all versions up to, and including, 1.0.5.1. This is due to insufficient escaping on the user-supplied parameter and lack of sufficient preparation on the existing SQL query - the value is split on `:` and both halves are interpolated directly into a `posts_where` SQL clause without `intval()` casting or `\$wpdb->prepare()`. This makes it possible for unauthenticated attackers to append additional SQL queries into the already-existing query that can be used to extract sensitive information from the database (researcher demonstrated extraction of database(), wp_users.user_login, and wp_users.user_pass).	2026-08-05	7.5	CVE-2026-18881
Red Hat-- Multicluster Engine for Kubernetes	A flaw was found in the Multicluster Engine for Kubernetes ClusterCurator controller. A tenant administrator with namespace-scoped privileges can exploit this vulnerability by creating a namespaced ClusterCurator. This action inadvertently grants the tenant administrator the ability to mint a token for a ServiceAccount with cluster-wide administrative authority. This leads to a privilege escalation, allowing the tenant administrator to gain full control over the cluster.	2026-08-05	9.1	CVE-2026-10059
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the Application Subscription controller (multicluster-operators-subscription) of Red Hat Advanced Cluster Management for Kubernetes (ACM). A user with namespace-scoped "edit" privileges in an ACM hub namespace can create a Channel resource pointing to a Helm repository they control and a Subscription resource referencing it. The app-subscription controller fetches and applies the Helm chart contents with its own elevated authority, without verifying whether the subscription creator holds the "open-cluster-management:subscription-admin" role and without restricting applied resources to the subscription namespace. This allows the attacker to include cluster-scoped resources in the Helm chart, such as a ClusterRoleBinding granting the attacker's ServiceAccount the "cluster-admin" ClusterRole. Successful exploitation results in	2026-08-05	9.9	CVE-2026-10090

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	full cluster-admin privilege escalation. This contradicts the ACM documentation which states that non-subscription-admin users should have resources deployed into the subscription namespace only.			
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in Keycloak's Dynamic Client Registration (DCR) security policy management. The "Allowed Protocol Mapper Types" policy, which restricts which types of data mappers a client can use, fails to re-validate the mapper type during a client update if the mapper's configuration remains unchanged. An attacker with client registration privileges can exploit this by first registering an allowed mapper type with a malicious configuration and then swapping it for a restricted, high-privilege mapper type (such as one that hardcodes administrative roles). This allows the attacker to gain full administrative access to the Keycloak realm.	2026-08-05	8.8	CVE-2026-15572
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in Keycloak's Authorization Services. The component responsible for matching request paths to security policies (PathMatcher) does not properly normalize URIs before comparison. By adding extra characters like a trailing slash or matrix parameters to a URL, an attacker can trick the system into applying a less restrictive security policy than intended. This allows an authenticated user to access administrative or restricted areas they should not have permission to see.	2026-08-05	8.1	CVE-2026-15573
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in the Dynamic Client Registration (DCR) component of Keycloak, an identity and access management solution. The default DCR policy fails to properly validate the claim path for User Property mappers, allowing them to write values to sensitive internal claim locations. An attacker with a standard user account and a limited Initial Access Token can exploit this to forge administrative roles in their access token. This allows the attacker to take over other clients, steal confidential secrets, and potentially gain full administrative control over the realm.	2026-08-05	8.1	CVE-2026-16102
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in the SAML broker component of Keycloak, which is used to manage identity federation and user authentication. The issue occurs because the IdP-initiated Single Sign-On endpoint fails to check if a provider is restricted to account linking only. This allows an attacker with control over a linked upstream identity to bypass login restrictions and gain full access to a local user account.	2026-08-05	7.4	CVE-2026-16442
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in the SAML metadata import functionality of the keycloak-services component, which is the core engine for identity brokering in Red Hat Build of Keycloak. When importing identity provider metadata that lacks specific usage attributes for keys, the system incorrectly disables signature validation for SAML responses even if a signing certificate is provided. This issue allows an unauthenticated attacker to forge a SAML response and gain unauthorized access to a user account by knowing their external identifier.	2026-08-05	7.4	CVE-2026-16443
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in dracut. The die() error-handling function writes its message into a shell script under the initramfs emergency-hook directory without properly shell-quoting it. When the message contains data derived from the DHCP ROOT_PATH option, an attacker on the adjacent network who controls a rogue DHCP server can inject a command-substitution sequence that executes as root the next time dracut sources its emergency hook scripts during standard boot-failure handling.	2026-08-07	7.5	CVE-2026-15816
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the GStreamer gst-plugins-good package. The rtph264depay and rtph265depay RTP depayloader elements do not enforce a maximum size limit on the reassembly buffer used during fragmented RTP packet processing. A remote, unauthenticated attacker can send a continuous stream of RTP fragments without ever transmitting an end-of-fragment marker, causing the reassembly buffer to grow without bound until process memory is exhausted. This results in a denial of service through process termination.	2026-08-06	7.5	CVE-2026-18649
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in udisks2. A local attacker with an active console session can exploit insufficient authorization checking on the 'as-user' option in the org.freedesktop.UDisks2.Filesystem.Mount() D-Bus method. This allows the attacker to spoof the 'as-user' parameter, mounting filesystems on behalf of arbitrary users, including privileged accounts. This can lead to local privilege escalation through mount point injection and manipulation of the mount namespace visible to privileged users.	2026-08-06	7.8	CVE-2026-7867
Red Hat--Red Hat Enterprise Linux 6	A heap-based buffer overflow vulnerability exists in the GIMP DDS (DirectDraw Surface) file parser. When a crafted DDS file declares a D3D9 pixel format but sets a lower bits-per-pixel (bpp) value in the header, the loader allocates an undersized heap buffer. Subsequent pixel data consumption at the real format's stride causes a write past the heap buffer boundary, leading to heap metadata corruption and potential code execution.	2026-08-08	7.8	CVE-2026-42170

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 9	A heap-buffer-overflow vulnerability exists in the APNG (Animated PNG) file loader of GIMP. This flaw occurs when the `fcTL` width exceeds the `IHDR` width, leading to pixel data being written past the end of a heap allocation. Additionally, a heap-based buffer overflow exists in the DDS plug-in due to a BPP mismatch in the `load_layer()` function. Both vulnerabilities can be triggered by opening a specially crafted image file, potentially leading to code execution.	2026-08-04	7.3	CVE-2026-42169
Rongzhitong--Visual Integrated Command and Dispatch Platform	A vulnerability was detected in Rongzhitong Visual Integrated Command and Dispatch Platform up to 20260617. Impacted is an unknown function of the file /dm/dispatch/userinfo/upload. Performing a manipulation of the argument File results in unrestricted upload. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	7.3	CVE-2026-18969
Rongzhitong--Visual Integrated Command and Dispatch Platform	A flaw has been found in Rongzhitong Visual Integrated Command and Dispatch Platform up to 20260617. The affected element is an unknown function of the file /dm/dispatch/user/findAll. Executing a manipulation of the argument Name can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	7.3	CVE-2026-18970
rxii--microtar	microtar's mtar_write_file_header() and mtar_write_dir_header() functions (src/microtar.c) copy a caller-supplied entry name into the 100-byte `name` field of a stack-allocated mtar_header_t via strcpy(h.name, name), with no check that strlen(name) is less than 100 before the copy. Any application that calls these functions with an externally-influenced filename longer than 99 characters (e.g. when archiving user-supplied or attacker-controlled filenames) triggers a stack buffer overflow.	2026-08-05	9.8	CVE-2026-71267
saadiqbal--WPFormify Stripe Payments with Form and Checkout	The WPFormify - Stripe Payments with Form and Checkout plugin for WordPress is vulnerable to unauthorized modification and deletion of Stripe payment credentials in all versions up to, and including, 1.1.1. This is due to missing capability checks and nonce verification on the `wpf_stripe_callback_success()` and `wpf_stripe_disconnect()` functions, both hooked to `admin_init`. The `admin_init` hook fires on `admin-post.php` which is accessible without authentication. This makes it possible for unauthenticated attackers to overwrite the site's Stripe API credentials with attacker-controlled values (redirecting payments to the attacker's Stripe account) or disconnect the Stripe integration entirely by deleting the stored credentials.	2026-08-05	8.2	CVE-2026-6627
Sangfor--Operation and Maintenance Security Management System	A vulnerability was determined in Sangfor Operation and Maintenance Security Management System up to 3.0.13. Affected by this vulnerability is the function com.sbr.fort.foreignDP.DpLoginController of the file /fort/portal_login of the component Login Endpoint. This manipulation causes os command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	7.3	CVE-2026-18641
Scott Paterson--Easy PayPal Buy Now Button	Unauthenticated Cross Site Scripting (XSS) in Easy PayPal Buy Now Button <= 2.0.4 versions.	2026-08-06	7.1	CVE-2026-65517
Scripta--eScriptorium	Authorization bypass in the Line, LineTranscription, VirtualCollection, tag and process API endpoints in Scripta/eScriptorium through 26.04.1 allows a remote authenticated user to read, modify and delete other users' transcription content via primary keys supplied in the request body, which are queried against the global model manager instead of the request-scoped queryset	2026-08-06	8.8	CVE-2026-18258
Scripta--eScriptorium	Server-side request forgery in the METS and IIIF import URI handling in Scripta eScriptorium through 26.04.1 allows a remote authenticated user to make the server issue arbitrary HTTP requests to internal hosts, including the cloud instance metadata service, via the mets_uri or iiif_uri parameter of POST /api/documents/{pk}/imports/, because the IMPORT_ALLOWED_DOMAINS setting defaults to '*' and no address filtering, redirect cap or timeout is applied	2026-08-06	8.5	CVE-2026-18359
Scripta--eScriptorium	Missing authorization in the OcrModelRight create and delete views in Scripta eScriptorium through 26.04.1 allows a remote authenticated user to grant themselves access to another user's private OCR model and to revoke any user's OCR model access via a POST request, because the ownership check is placed in get_context_data() and therefore runs only on the GET rendering path	2026-08-06	7.1	CVE-2026-18277
SecureAge--CatchPulse	An improper access control vulnerability in CatchPulse could allow a non-administrative local-attacker to connect to an unrestricted kernel filter communication port and bypass CatchPulse's security policy enforcement.	2026-08-06	8.4	CVE-2026-55978

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SEO Squirrly--SEO Plugin by Squirrly SEO	Unauthenticated Cross Site Scripting (XSS) in SEO Plugin by Squirrly SEO <= 14.2.0 versions.	2026-08-06	7.1	CVE-2026-66664
sequelize--sequelize	Sequelize is a Node.js ORM tool. Prior to 6.37.4, SQL injection is possible with strings only if dialect is set to oracle. The escape function defined in sql-string.js does not escape quotes if the value starts with TO_TIMESTAMP or TO_DATE. In the Oracle dialect, when val is a string and starts with TO_TIMESTAMP or TO_DATE, escape returns val directly instead of replacing single quotes. An attacker can inject arbitrary SQL expressions through an application value that reaches this escape path. This issue is fixed in version 6.37.4.	2026-08-03	9.8	CVE-2026-69240
Sergey--AIWU	Unauthenticated Privilege Escalation in AIWU <= 1.5.6 versions.	2026-08-06	9.8	CVE-2026-65507
sh1zen--Multi Uploader for Gravity Forms	The Multi Uploader for Gravity Forms plugin for WordPress is vulnerable to unauthorized arbitrary media deletion in all versions up to, and including, 1.1.8. This is due to missing capability checks in the `plupload_ajax_delete_file()` function, which is registered via `wp_ajax_nopriv_gfm_delete_file`. The nonce intended for CSRF protection is exposed on any public-facing page containing a multi-uploader form field via the `GFMU_options` JavaScript object. This makes it possible for unauthenticated attackers to permanently delete any WordPress media attachment by supplying its attachment ID, potentially leading to complete media library destruction.	2026-08-05	9.1	CVE-2026-5581
Shabti Kaplan--Frontend Admin by DynamiApps	Unauthenticated Privilege Escalation in Frontend Admin by DynamiApps <= 3.29.10 versions.	2026-08-06	9.8	CVE-2026-66662
Shabti Kaplan--Frontend Admin by DynamiApps	Subscriber Broken Access Control in Frontend Admin by DynamiApps <= 3.29.10 versions.	2026-08-06	7.1	CVE-2026-66470
Shandong Hoteam--PDM Product Data Management System	A vulnerability has been found in Shandong Hoteam PDM Product Data Management System up to 8.3.10. The impacted element is the function GetStoredClassByFilter of the file /Base/BaseService.asmx/DataService. The manipulation of the argument FilterString leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	7.3	CVE-2026-18854
Shenzhen Aitemi--M300 Wi-Fi Repeater	A security flaw has been discovered in Shenzhen Aitemi M300 Wi-Fi Repeater r0-ea7890a. Impacted is the function sprintf of the file /protocol.csp?fname=net&opt=smacfilter_conf&function=set&act=add&name=test&enable=1. Performing a manipulation of the argument enable/name/mac results in command injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	2026-08-09	9.8	CVE-2026-19348
Shibby--Tomato	A vulnerability was determined in Shibby Tomato 1.28.0000. Affected by this vulnerability is the function new_qoslimit_stop of the file /tmp/qoslimittc_stop.sh. Executing a manipulation of the argument wan_iface can lead to os command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This project is superseded by FreshTomato.	2026-08-06	7.2	CVE-2026-19034
Shibby--Tomato	A vulnerability was identified in Shibby Tomato 1.28.0000. Affected by this issue is the function new_qoslimit_start of the file /etc/qoslimit. The manipulation of the argument new_qoslimit_enable leads to os command injection. The attack may be initiated remotely. The exploit is publicly available and might be used. This project is superseded by FreshTomato.	2026-08-06	7.2	CVE-2026-19035
Shibby--Tomato	A security flaw has been discovered in Shibby Tomato 1.28.0000. This affects the function sub_40F88C of the file /tmp/ppp/wanoptions. The manipulation of the argument ppp_custom results in os command injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. This project is superseded by FreshTomato.	2026-08-06	7.2	CVE-2026-19036
siyuan-note--siyuan	SiYuan versions before v3.7.3 contain SQL injection vulnerabilities in the fullTextSearchAssetContent endpoint reachable by unauthenticated users and publish RoleReader tokens. Attackers can execute arbitrary SQL on the read-write asset-content database via unescaped method parameters and REGEXP clauses to read, modify, or delete cross-notebook data.	2026-08-03	10	CVE-2026-69083
siyuan-note--siyuan	SiYuan versions <= v3.7.2 expose the /api/search/searchEmbedBlock endpoint, which passes a client-supplied SQL statement verbatim to the main read-write siyuan.db handle with no single-statement, read-only, or admin restrictions. The endpoint is gated only by CheckAuth, making it reachable by the publish RoleReader token and by anonymous users when publish authentication is	2026-08-03	10	CVE-2026-69084

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disabled. Because the underlying driver executes stacked statements, an attacker can read and modify content across all opened cleartext notebooks (encrypted per-box notebooks are excluded). Fixed in v3.7.3.			
siyuan-note--siyuan	SiYuan before v3.7.3 contains a SQL injection vulnerability in the /api/filetree/searchDocs endpoint, where the caller-supplied keyword parameter is concatenated directly into SQL statements with no escaping or parameter binding. The endpoint is reachable by a publish RoleReader token, or unauthenticated when publish mode is enabled with Publish.Auth.Enable set to false. Because the statement executes on a read-write SQLite handle via a driver that supports stacked (semicolon-separated) statements, an attacker can read and modify database content across all cleartext (non-encrypted) notebooks on the instance.	2026-08-03	10	CVE-2026-69085
siyuan-note--siyuan	SiYuan versions before v3.7.3 contain an authentication bypass vulnerability in publish mode where content-returning endpoints getHeadingChildrenDOM, getHeading*Transaction, and getBacklinkDoc perform no password check despite protecting the primary getDoc endpoint. Anonymous attackers can retrieve full content of password-protected documents by obtaining internal block IDs from reader-accessible endpoints and calling unprotected content endpoints to bypass the password gate.	2026-08-03	8.6	CVE-2026-68584
siyuan-note--siyuan	SiYuan before v3.7.3 fails to apply publish-access filters to the getBacklinkDoc and getBackmentionDoc content endpoints (/api/ref/getBacklinkDoc and /api/ref/getBackmentionDoc). While the corresponding backlink list endpoints filter publish-forbidden documents, the content endpoints (gated only by CheckAuth) do not. A publish-mode reader - including an anonymous reader when publish Basic Auth is disabled - can call these endpoints directly with a publish-forbidden document's ID to retrieve its rendered DOM content and to determine whether the document references a given block (a reference-existence oracle).	2026-08-03	8.6	CVE-2026-68586
siyuan-note--siyuan	SiYuan versions before v3.7.3 contain an information disclosure vulnerability in the getHeadingDeleteTransaction, getHeadingLevelTransaction, and getHeadingInsertTransaction endpoints that return rendered block DOM without publish-access checks. Anonymous readers or publish RoleReader tokens can supply a heading block ID to read full rendered content of publish-disabled documents that should be restricted.	2026-08-03	8.6	CVE-2026-68587
siyuan-note--siyuan	SiYuan versions before v3.7.3 fail to validate the avID parameter on all code branches in attribute-view read endpoints, allowing attackers to construct traversal paths that escape the storage directory. Authenticated users with RoleReader permissions or anonymous clients when publish authentication is disabled can read JSON files outside the attribute-view directory to disclose cross-scope database content.	2026-08-03	7.7	CVE-2026-69086
socketio--socket.io	Socket.IO enables bidirectional and low-latency communication for every platform. Prior to 4.2.7, 3.4.5, and 3.3.6, a specially crafted Socket.IO packet can make the server wait for a large number of binary attachments and buffer them, which can be exploited to make the server run out of memory. This vulnerability is fixed in 4.2.7, 3.4.5, and 3.3.6.	2026-08-03	7.5	CVE-2026-69185
Soflyy--Breakdance	Missing Authorization vulnerability in Soflyy Breakdance allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Breakdance: from n/a before 2.7.	2026-08-06	7.5	CVE-2026-65551
solutioned--Staff Training	Unauthenticated Broken Access Control in Staff Training <= 1.0.7 versions.	2026-08-06	7.3	CVE-2026-65541
Sophos--Sophos Endpoint for macOS	A privilege escalation vulnerability allows local users to execute arbitrary code as root via Sophos Endpoint for macOS older than version 2026.1.1 and Sophos Home for macOS older than version 10.11.6.	2026-08-06	9.3	CVE-2026-18367
SourceCodester--Computer Repair Shop Management System	A security vulnerability has been detected in SourceCodester Computer Repair Shop Management System 1.0. Affected by this issue is some unknown functionality of the file /classes/Master.php?f=delete_product. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	2026-08-06	7.3	CVE-2026-19021
SourceCodester--Photo Share Website	A vulnerability was found in SourceCodester Photo Share Website 1.0. The impacted element is an unknown function of the file /social/ajax.php?action=login. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	2026-08-07	7.3	CVE-2026-19196
SourceCodester--Photo Share Website	A vulnerability was found in SourceCodester Photo Share Website 1.0. This affects an unknown function of the file /social/ajax.php?action=signup. Performing a manipulation of the argument email results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2026-08-07	7.3	CVE-2026-19211

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Simple Doctors Appointment System	A security flaw has been discovered in SourceCodester Simple Doctors Appointment System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=delete_appointment. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-08-07	7.3	CVE-2026-19231
Spacebar Server--Spacebar Server	Spacebar Server before commit dcf910 contains a missing authorization vulnerability that allows any authenticated attacker to add themselves to arbitrary group DM channels by sending a PUT request to the channels recipient endpoint without membership verification. Attackers can exploit the unguarded PUT /channels/{channel_id}/recipients/{user_id} handler to join private group DMs, read complete message history, post messages as a participant, and force-add third-party users without their consent.	2026-08-05	8.1	CVE-2026-70617
StableBit--DrivePool	A security vulnerability has been detected in StableBit DrivePool 2.3.13.1687. This vulnerability affects unknown code of the file C:\Program Files\StableBit\DrivePool\DrivePool.Service.exe of the component DrivePoolService. Such manipulation leads to permission issues. The attack must be carried out locally. The exploit has been disclosed publicly and may be used.	2026-08-07	7.8	CVE-2026-19191
StableBit--Scanner	A weakness has been identified in StableBit Scanner 2.6.13.4088. This affects an unknown part of the file C:\Program Files (x86)\StableBit\Scanner\Service\Scanner.Service.exe of the component ScannerService. This manipulation causes permission issues. The attack is restricted to local execution. The exploit has been made available to the public and could be used for attacks.	2026-08-07	7.8	CVE-2026-19190
statamic--cms	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.74.1 and 6.24.0, when OAuth login was enabled with a provider that does not guarantee verified email addresses, an unauthenticated attacker could sign in as an existing user, potentially including a super admin, without knowing that user's password, because the application matched OAuth identities to accounts by email address alone. Exploitation requires OAuth to be explicitly enabled with such a provider. This issue is fixed in versions 5.74.1 and 6.24.0.	2026-08-06	8.1	CVE-2026-64665
stellarwp--Membership Plugin Kadence Memberships	The Membership Plugin - Kadence Memberships plugin for WordPress (formerly Restrict Content) is vulnerable to password reset link poisoning leading to account takeover in all versions up to, and including, 4.0.0. This is due to the legacy lost-password handler rc_process_lost_password_form() consuming the attacker-controlled rc_redirect POST parameter into two unvalidated sinks in legacy/includes/forms.php: wp_redirect(esc_url(\$_POST['rc_redirect'])) at line 243, and add_query_arg(array('key' => \$key, 'login' => ...), \$_POST['rc_redirect']) inside rc_send_password_reset_email() at line 306. The nonce required to reach the handler is broadcast by the public [login_form] shortcode at line 207 to any anonymous visitor. This makes it possible for unauthenticated attackers to issue a password-reset request for any account (including administrators) whose reset email body points the victim at an attacker-controlled host carrying a valid reset key/login. When the victim clicks the link, the reset key leaks to the attacker, who can replay it against the legitimate site to complete account takeover.	2026-08-05	9.3	CVE-2026-9273
Stephan Muelle--libkcapi	Memory Corruption via Uncanceled AIO Requests on Error: libkcapi's one-shot AIO path can return an error before all submitted IOCBs are drained, allowing later kernel writes into caller-owned output buffers.	2026-08-05	7.3	CVE-2026-71226
Stirling-Tools--Stirling-PDF	Stirling-PDF's POST /api/v1/convert/url/pdf endpoint (ConvertWebsiteToPDF.java) was not updated with the CustomHTMLSanitizer/SsrfProtectionService SSRF protections that were added to three sibling conversion endpoints (html/pdf, file/pdf, markdown/pdf). The endpoint validates only that the initial requested URL resolves to a public IP, then fetches the page's HTML server-side and hands it, unsanitized, to a WeasyPrint subprocess. Embedded resource references in the fetched HTML (e.g.) are fetched by WeasyPrint with no per-resource SSRF filtering, allowing an attacker-controlled page to cause the server to retrieve cloud metadata endpoints or internal network resources and leak their contents back into the generated PDF.	2026-08-05	8.6	CVE-2026-71270
supsysiticom--Smart Popup by Supsysitic	The Smart Popup by Supsysitic plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.12.0. This is due to a permission map collision in the `havePermissions()` function in `classes/frame.php`, where `array_merge()` overwrites the popup module's administrator-restricted method list with the base controller's value, silently removing `save` from protected actions; this is compounded by the subscription confirmation email embedding the	2026-08-05	8.8	CVE-2026-18322

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	same generic `pps_nonce` that the unauthenticated `wp_ajax_nopriv_save` endpoint accepts, and by the complete absence of any server-side role allowlist in `createWpSubscriber()`. This makes it possible for unauthenticated attackers to submit a crafted POST request to `admin-ajax.php` using a nonce obtained from a public subscription confirmation email, setting `params[tpl][sub_wp_create_user_role]` to `administrator` via the exposed `popupControllerPps::save()` action, and then triggering the stored confirmation flow to create a persistent WordPress Administrator account with attacker-chosen credentials.			
SUSE--NeuVector	NeuVector through 5.4.9 is can potentially leak information from manager /network/graph API due to missing authentication and cached data containing sensitive information.	2026-08-05	7.3	CVE-2026-25703
SUSE--Rancher	A privilege escalation vulnerability exists in Rancher's impersonation middleware (pkg/auth/requests/impersonate.go). An authenticated Rancher user with the default user global role can gain full administrative access to the Rancher control plane and transitively to all downstream clusters it manages. This issue affects Rancher: from 2.11.0 before 2.11.16, from 2.12.0 before 2.12.12, from 2.13.0 before 2.13.8, and from 2.14.0 before 2.14.2.	2026-08-05	9.1	CVE-2026-44945
SUSE--Rancher	When API audit logging is enabled, the middleware reads the entire HTTP request body into memory without enforcing a size limit on login endpoints. Because the audit middleware is positioned earlier in the handler chain than Rancher's APIBodyLimitingHandler, the body-size cap (default 1 MiB) is bypassed for requests that pass through the audit copyReqBody path. An unauthenticated attacker can send arbitrarily large request bodies to the public login endpoints, causing the Rancher Manager server process to allocate memory proportional to the supplied body size. With just a few concurrent connections, this can exhaust available memory and terminate the Rancher Manager plane process, making the Rancher API and UI unavailable and interrupting management of all downstream clusters.	2026-08-05	7.5	CVE-2026-59675
Swiss Federal Office of Information Technology, Systems and Telecommunication--@oblique/cli	@oblique/cli 15.4.0 contains an OS command injection vulnerability in the project creation functionality. The CLI constructs shell commands through string concatenation and executes them with execSync(). A user-controlled project-name argument is inserted into the shell command without proper neutralization, allowing shell metacharacters to execute additional operating-system commands when the CLI is invoked with a crafted project name.	2026-08-05	7.8	CVE-2026-16022
Syed Balkhi--NextGEN Gallery	Unauthenticated Cross Site Scripting (XSS) in NextGEN Gallery <= 4.2.3 versions.	2026-08-06	7.1	CVE-2026-28141
Synology--Synology Assistant	An incorrect default permissions vulnerability in Synology Assistant before 7.0.7-50095 allows local users to read or write arbitrary files and conduct denial-of-service during installation.	2026-08-03	7.3	CVE-2026-4793
syoyo--tinyobjloader-c	tinyobjloader-c's tinyobj_parse_and_index_mtl_file() (tinyobj_loader_c.h) reads each line of a .mtl material file into a fixed 4096-byte stack buffer `linebuf` via memcpy(linebuf, p, p_len), guarded only by `assert(p_len < 4095)`. Because assert() compiles to a no-op under -DNDEBUG (standard for release builds), a crafted .mtl file containing a line (e.g. a "newmtl" material name) longer than 4096 bytes overflows linebuf into the adjacent stack variable namebuf and beyond, corrupting the stack of any application that loads attacker-supplied 3D model/material files. The identical vulnerable pattern is duplicated in a second function in the same file.	2026-08-05	7.8	CVE-2026-71266
TBTAK BLGEM Software Technologies Research Institute--pardus-image-writer	External control of file name or path vulnerability in TÃfÃ“BÃ„Ã°TAK BÃ„Ã°LGEM Software Technologies Research Institute pardus-image-writer allows Removing Important Client Functionality. This issue affects pardus-image-writer: before 1.0.4.	2026-08-04	7.1	CVE-2026-18806
Telenia Software--TVox	Telenia Software TVox 26.5.3 and prior 26.x versions, and 24.9.21 and prior 24.x versions, contain an authentication bypass vulnerability in set_env.php where the redirectToLoginAdminRequestHaveAccessToken() function derives the current page name from PHP_SELF and skips authentication when the value matches 'login_admin.php'. Attackers can append '/login_admin.php' to the path of any target PHP script to cause the authentication check to pass and gain unauthenticated access to all PHP scripts under the manager HTML directory.	2026-08-03	9.8	CVE-2026-64827
Telenia Software--TVox	Telenia Software TVox 26.5.3 and prior 26.x versions, and 24.9.21 and prior 24.x versions, contain an OS command injection vulnerability in action_audio.php that	2026-08-03	7.2	CVE-2026-67608

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows authenticated attackers to execute arbitrary operating system commands by passing an unsanitized pid parameter into an exec() call when the action parameter is set to checkProcess. Attackers can inject malicious OS commands through the pid request parameter to execute arbitrary commands with the privileges of the apache user.			
Telenia Software--TVox	Telenia Software TVox 26.5.3 and prior 26.x versions, and 24.9.21 and prior 24.x versions, contain a privilege escalation vulnerability that allows attackers with access to the apache account to execute arbitrary commands as root by exploiting an insecure sudoers configuration in /etc/sudoers.d/telenia. The configuration grants the apache user NOPASSWD execution of /bin/nice, which can be leveraged to invoke arbitrary commands, enabling full root-level command execution without supplying a password.	2026-08-03	7.8	CVE-2026-67609
Tenable, Inc.--Sensor Proxy	A vulnerability in Tenable Sensor Proxy allows a remote attacker to execute code with elevated privileges by inducing an operator to connect the sensor to an attacker-controlled host.	2026-08-03	9.6	CVE-2026-18667
Tenda--CH22	A vulnerability was determined in Tenda CH22 1.0.0.1. This vulnerability affects the function formCertListInfo of the file /goform/CertListInfo. This manipulation of the argument Name causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-09	8.8	CVE-2026-19346
thebradleysanders--IOTSmartHome	IOTSmartHome's gui/login.php checkCookie() function builds an authentication query as SELECT * FROM users WHERE ID='<decoded lastLogin cookie>' after base64-decoding the client-supplied lastLogin cookie via safe_decode(), which performs URL-safe base64 decoding with no sanitization of the decoded value before it is concatenated into the SQL string. An unauthenticated attacker can set a lastLogin cookie containing a base64-encoded SQL injection payload (e.g. base64('' OR '1'='1')) to bypass authentication and, via UNION-based injection, extract arbitrary data including user credentials.	2026-08-05	9.8	CVE-2026-71231
ThemeREX--Abelle	Unauthenticated PHP Object Injection in Abelle <= 1.22 versions.	2026-08-06	9.8	CVE-2026-65573
themeruby--Easy Post Submission Frontend Posting, Guest Publishing & Submit Content for WordPress	The Easy Post Submission plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `create_post()` function in all versions up to, and including, 2.3.0. This is due to the `rbsm_submit_post` AJAX action being registered for unauthenticated users via `wp_ajax_nopriv_rbsm_submit_post` without any authorization checks when a `postId` parameter is supplied. This makes it possible for unauthenticated attackers to modify the title, content, excerpt, categories, and tags of arbitrary posts, as well as change the post status to draft (effectively unpublishing them) via the `postId` parameter.	2026-08-05	9.1	CVE-2026-4431
themetechmount--TrueBooker Appointment Booking and Scheduler System	The TrueBooker - Appointment Booking and Scheduler System plugin for WordPress is vulnerable to account takeover via improper password reset validation in all versions up to, and including, 1.2.3. This is due to the plugin not properly validating a user's identity before resetting their password. This makes it possible for unauthenticated attackers to reset the password of arbitrary user accounts, including administrators, and gain access to those accounts.	2026-08-07	9.8	CVE-2026-14364
themetechmount--TrueBooker Appointment Booking and Scheduler System	The TrueBooker - Appointment Booking and Scheduler System plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.2.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to change the password of arbitrary user accounts, including administrators, which can be leveraged to gain access to those accounts.	2026-08-07	9.8	CVE-2026-14365
theotherphil--imagecli	imagecli's `scale <ratio>` pipeline operation (Scale::apply() in src/image_ops.rs) computes output width/height as (dimension as f32 * ratio) as u32 with no upper-bound validation on the CLI-supplied ratio, which is parsed via nom::number::complete::float with no range check. A large ratio (e.g. 100000) causes an attempted allocation of hundreds of terabytes, aborting the process. Any application embedding imagecli as a library and accepting user-controlled pipeline strings is remotely crashable with a single request.	2026-08-05	7.5	CVE-2026-70377
theotherphil--imagecli	imagecli's `carve <ratio>` pipeline operation (Carve::apply() in src/image_ops.rs) only asserts `ratio <= 1.0`, never validating that the ratio is positive. A negative ratio (e.g. -5) causes the computed target width to saturate to 0 via Rust's defined float-to-uint cast, which is then passed to imageproc::seam_carving::shrink_width - a function that panics when given a width below 2, crashing the process. This shares the same missing-input-validation root cause as the sibling `scale` finding in the same file but is an independently fixable, distinct code path.	2026-08-05	7.5	CVE-2026-70378

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
thephleague--commonmark	league/commonmark is a PHP library for parsing and rendering CommonMark Markdown. From 0.6.0 until 2.9.0, specially crafted Markdown lines can cause the parser to have quadratic time complexity when converting, because several parsing paths repeatedly rescan growing portions of a line to translate between character positions and byte positions, and the Autolink extension can also copy and validate the remaining line at every URL-like prefix, allowing an attacker who can submit Markdown for conversion to consume disproportionate CPU time with a comparatively small request. This issue is fixed in 2.9.0.	2026-08-06	7.5	CVE-2026-71488
Thermo Fisher--Applied Biosystems 3500/3500xL Series Data Collection Software	The affected Thermo Fisher Applied Biosystems Genetic Analyzers are vulnerable because .fsa/.hid output files can be edited. An attacker could tamper with these files, altering DNA data and resulting in inaccurate DNA test outcomes.	2026-08-05	8.4	CVE-2026-17583
thiagoralves--OpenPLC_v3	OpenPLC Runtime v3's compile_program() function (webserver/openplc.py) parses `(*FILE:path content*)` directives from uploaded Structured Text (.st) program files and writes the referenced content to `os.path.join('./core', file_path)` with no validation that file_path stays within the ./core directory. A crafted .st file containing a directive such as `(*FILE:../../../../etc/cron.d/x * * * * root <command>*)` writes attacker-controlled content to an arbitrary filesystem path, enabling remote code execution (e.g. via cron or SSH authorized_keys). A path-validation function, validate_file_path(), exists elsewhere in the codebase (webserver/credentials.py) but is never invoked from compile_program(), leaving the sink unprotected. OpenPLC additionally ships with hardcoded default credentials (openplc:openplc), lowering the practical bar for exploitation.	2026-08-05	9.9	CVE-2026-71268
thomaspoignant--scim-patch	`scim-patch`, a library to perform SCIM patch, prior to version 0.9.1 performs prototype pollution when applying a SCIM PATCH operation whose `value` object contains a key like `""__proto__someProp""`. After one such patch, `Object.prototype.someProp` is set process-wide, affecting every plain object in the Node process. Any service that calls `scimPatch()` on attacker-controlled JSON (i.e. any SCIM endpoint accepting `PATCH` from an external IdP) is exploitable on a stock Node runtime. Version 0.9.1 contains a patch. A workaround is available. Calling `Object.freeze(Object.prototype)` (and the same on `Array.prototype`, `Function.prototype`) at process startup neutralizes this class of bug - assignment to a frozen prototype becomes a silent no-op in sloppy mode or a `TypeError` in strict mode. Node's `--frozen-intrinsics` flag does this for built-ins automatically.	2026-08-07	9.1	CVE-2026-48170
Thrive Themes Coupon--Thrive Architect	Unauthenticated Cross Site Scripting (XSS) in Thrive Architect <= 10.9.3.1 versions.	2026-08-06	7.1	CVE-2026-66694
timescale--timescaledb	TimescaleDB through 2.29.1, fixed in commit 517c13e, contains an out-of-bounds read in the Dictionary compression reverse row iterator (tsl/src/compression/algorithms/dictionary.c). The forward path validates the decoded index; the reverse path uses an assertion compiled out of release builds, leaving the 64-bit Simple8b index unvalidated and the read offset attacker-controlled. Attackers with DML access to a physical compressed relation can store a crafted datum and run a reverse-order scan. With a pass-by-value column type the out-of-bounds Datum is returned to the client as a normal column value, disclosing backend memory including the shared buffer pool, which SQL access control does not cover.	2026-08-06	8.1	CVE-2026-70634
timescale--timescaledb	TimescaleDB through 2.29.1, fixed in commit 517c13e, contains an out-of-bounds read vulnerability that allows authenticated attackers to cause query-result integrity failures or backend crashes by supplying a crafted Simple8b selector-11 value, which is stored in the signed int16 Arrow dictionary-index type and bypasses index validation checks in bulk text dictionary decompression. Attackers with direct DML access to a non-frozen physical compressed hypertable relation can trigger an out-of-bounds read before the base of the live offsets array through the VectorAgg single-text hashing strategy, resulting in incorrect aggregation output, backend SIGSEGV, or PostgreSQL crash recovery depending on build configuration.	2026-08-06	7.1	CVE-2026-70635
TinyAGI--TinyAGI	A weakness has been identified in TinyAGI 0.0.20. This issue affects the function collectFiles of the file packages/core/src/response.ts of the component Message API Endpoint. This manipulation causes file inclusion. The attack can be initiated remotely. The exploit has been made available to the public and could be used for	2026-08-06	7.3	CVE-2026-19009

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacks. The project was informed of the problem early through an issue report but has not responded yet.			
TinyAGI--TinyAGI	A security vulnerability has been detected in TinyAGI 0.0.20. Impacted is the function processMessage of the file packages/main/src/index.ts of the component Message API Endpoint. Such manipulation leads to missing authorization. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	7.3	CVE-2026-19010
treeverse--lakeFS	lakeFS is an open-source tool that transforms object storage into a Git-like repositories. Prior to version 1.81.1 of the open source edition and 1.84.0 of the enterprise edition, lakeFS Web UI renders markdown files from repository objects without sanitizing the resulting HTML. A user with write access to any repository branch can commit a `.md` object containing arbitrary HTML/JavaScript. Any other user who opens that object, or who navigates to a repository or directory containing a malicious `README.md`, executes the attacker-supplied script in their own authenticated session. lakeFS fixes the issue in v1.81.1 and lakeFS Enterprise fixes the issue in in v1.84.0. Enterprise customers using older versions can temporarily disable Markdown rendering by adding YAML to their config. No workaround exists for OSS release. Users are advised to upgrade to the latest version for both lakeFS and lakeFS-Enterprise.	2026-08-07	8.7	CVE-2026-48026
Trilby Media--grav-plugin-scheduler-webhook	Grav CMS's scheduler-webhook plugin contains an authentication bypass in the webhook token check. When the webhook feature is enabled but no webhookToken is configured, a compound conditional short-circuits and skips token validation, so an unauthenticated remote attacker who can reach POST /scheduler/webhook can trigger the operator's already-configured scheduled jobs by sending a single request. The primitive is triggering-existing-jobs, not attacker-chosen command execution: the attacker controls when the jobs run and which one runs (via ?job=), but does not control what the jobs do. Code execution follows only when the operator has configured a job that shells out, and even then the attacker controls timing rather than payload. Not a default-install issue: reaching the endpoint requires the separate scheduler-webhook GPM plugin to be installed, scheduler.modern.webhook.enabled to be true (default false), and no webhookToken to be configured; a stock Grav or Grav-Admin install exposes nothing here.	2026-08-07	7.3	CVE-2026-11430
Trippo--ResponsiveFileManager	A security flaw has been discovered in Trippo ResponsiveFileManager up to 9.14.0. The impacted element is an unknown function of the file filemanager/dialog.php. The manipulation results in unrestricted upload. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	2026-08-04	7.3	CVE-2026-18788
TUBITAK BILGEM Software Technologies Research Institute--eta-otp-lock	Deserialization of untrusted data vulnerability in TUBITAK BILGEM Software Technologies Research Institute eta-otp-lock allows Object Injection. This issue affects eta-otp-lock: before 1.0.4.	2026-08-03	7.8	CVE-2026-18642
tychesoftware--Order Delivery Date for WooCommerce	Shop manager Privilege Escalation in Order Delivery Date for WooCommerce <= 4.6.0 versions.	2026-08-06	7.2	CVE-2026-65559
typemill--typemill	Typemill's login endpoint (POST /tm/login, ControllerWebAuth::login()) performs no rate-limiting, failed-attempt counting, or account lockout when captcha is disabled, which is the default configuration. An unauthenticated attacker can send unlimited password-guessing requests against any account, including administrators, with no throttling. The only attempt-counting/lockout logic present in the same file protects an optional secondary email-authcode step and does not apply to the primary password check.	2026-08-05	9.1	CVE-2026-71213
Uasoft--Badaso	A vulnerability has been found in Uasoft Badaso 3.0.0-alpha. This vulnerability affects the function ApiRequest::class of the file src/Routes/api.php of the component File API. The manipulation leads to permission issues. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	7.3	CVE-2026-19376

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Unisoc (Shanghai) Technologies Co., Ltd.--T8100/T9100/T8200/T8300	In nr modem, there is a possible improper input validation. This could lead to remote denial of service with System execution privileges needed.	2026-08-03	7.5	CVE-2026-21548
Unisoc (Shanghai) Technologies Co., Ltd.--T8100/T9100/T8200/T8300	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	2026-08-03	7.5	CVE-2026-21549
Unisoc (Shanghai) Technologies Co., Ltd.--T8100/T9100/T8200/T8300	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	2026-08-03	7.5	CVE-2026-21550
Unisoc (Shanghai) Technologies Co., Ltd.--T8100/T9100/T8200/T8300	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	2026-08-03	7.5	CVE-2026-21551
Unisoc (Shanghai) Technologies Co., Ltd.--T8100/T9100/T8200/T8300	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	2026-08-03	7.5	CVE-2026-21552
Unisoc (Shanghai) Technologies Co., Ltd.--T8100/T9100/T8200/T8300	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	2026-08-03	7.5	CVE-2026-21553
Unisoc (Shanghai) Technologies Co., Ltd.--UDX710	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	2026-08-03	7.5	CVE-2026-21554
Unisoc (Shanghai) Technologies Co., Ltd.--UDX710	In modem, there is a possible improper input validation. This could lead to remote denial of service with no additional execution privileges needed	2026-08-03	7.5	CVE-2026-21555
usememos--memos	Memos' webhook URL validation, isReservedIP() (internal/webhook/validate.go), checks a candidate IP against a reservedCIDRs list that omits 0.0.0.0/8 and never calls ip.IsUnspecified() - unlike the correctly implemented sibling function isInternalIP() in internal/httpgetter/html_meta.go, which does. Because Linux redirects connections to 0.0.0.0 to loopback (127.0.0.1), an attacker registering a webhook URL of http://0.0.0.0:PORT/ bypasses the reserved-IP check and causes the Memos server to make outbound HTTP requests to its own loopback interface, exposing internal-only services.	2026-08-05	8.5	CVE-2026-71271
usememos--memos	Memos' webhook dispatch function safeDialContext() (internal/webhook/webhook.go) resolves the target hostname via net.DefaultResolver.LookupHost() and validates the resulting IPs against reserved ranges, but then dials net.JoinHostPort(host, port) using the original hostname rather than the already-validated IP address. Because net.Dialer.DialContext() performs its own independent DNS resolution, an attacker controlling DNS for the webhook's hostname (e.g. via a short TTL) can return a public, allowed IP during validation and a different, internal IP at dial time - a classic time-of-check/time-of-use DNS-rebinding bypass of the SSRF protection.	2026-08-05	8.5	CVE-2026-71272
UTT--HiPER 1200GW	A security flaw has been discovered in UTT HiPER 1200GW up to v2.5.3-170306. This affects the function strcpy of the file /goform/ConfigAdvideo. The manipulation of the argument timestart results in stack-based buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	8.8	CVE-2026-18898
UTT--HiPER 1200GW	A security vulnerability has been detected in UTT HiPER 1200GW up to 2.5.3-170306. This impacts the function strcpy of the file /goform/pptpSrvGlobalConfig. Such manipulation of the argument EncryptionMode leads to stack-based buffer overflow. The attack can be executed remotely. The exploit has been disclosed	2026-08-09	8.8	CVE-2026-19341

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
UTT--HiPER 1250GW	A vulnerability was found in UTT HiPER 1250GW up to 3.2.7-210907-180535. Impacted is the function strcpy of the file /goform/APSecurity_5g. Performing a manipulation of the argument cipher results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	8.8	CVE-2026-18895
UTT--HiPER 1250GW	A vulnerability was identified in UTT HiPER 1250GW up to v3.2.7-210907-180535. The impacted element is the function strcpy of the file /goform/getOneApConfTempEntry. The manipulation of the argument tempName leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	8.8	CVE-2026-18897
V-Secure--Jingyun Antivirus	A vulnerability has been found in V-Secure Jingyun Antivirus 2.4.2.39. The affected element is an unknown function in the library ZyArk.sys of the component Kernel Driver. The manipulation leads to improper access controls. The attack needs to be performed locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-07	7.8	CVE-2026-19195
vibesurf-ai--VibeSurf	A vulnerability has been found in vibesurf-ai VibeSurf up to cd6e519d507cdd4d63061300bf60fb176e1f57e0. Impacted is an unknown function of the file /code of the component Python Validation Handler. The manipulation leads to code injection. Remote exploitation of the attack is possible. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	7.3	CVE-2026-18770
vimeodev--Vimeo	Subscriber Sensitive Data Exposure in Vimeo <= 1.2.2 versions.	2026-08-06	7.5	CVE-2026-65543
vovchic17--aiosend	aiosend is a synchronous and asynchronous Crypto Pay API client. Prior to version 3.0.7, 'WebhookHandler.feed_update()' deserializes the entire request body before verifying the HMAC signature. This allows an unauthenticated attacker to force expensive parsing of arbitrary JSON payloads that will ultimately be rejected, leading to unnecessary CPU and memory consumption. Version 3.0.7 fixes the issue. Some workarounds are available. Restrict request body size at the reverse proxy or web framework, rate-limit webhook endpoints, and/or reject oversized requests before JSON parsing.	2026-08-06	7.5	CVE-2026-70646
Wavlink--WL-NU516U1	A vulnerability has been found in Wavlink WL-NU516U1 708c073-mt7628. This affects the function fgets of the file nas.cgi. The manipulation of the argument CONTENT_LENGTH leads to stack-based buffer overflow. Remote exploitation of the attack is possible. You should upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-08-03	9.8	CVE-2026-18588
Wavlink--WL-NU516U1	A vulnerability was found in Wavlink WL-NU516U1 708c073-mt7628. This impacts the function change_password of the file nas.cgi. The manipulation of the argument User1Passwd results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used. The affected component should be upgraded. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-08-03	9.8	CVE-2026-18589
Wavlink--WL-NU516U1	A flaw has been found in Wavlink WL-NU516U1 708c073-mt7628. The impacted element is an unknown function of the component Config Import. Executing a manipulation of the argument Password can lead to os command injection. The attack may be launched remotely. This attack is characterized by high complexity. The exploitability is regarded as difficult. The exploit has been published and may be used. It is advisable to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-08-03	7.5	CVE-2026-18587
Wavlink--WN572	A security vulnerability has been detected in Wavlink WN572, WN570H, WN573, WN529, WN530, WN531, WN535, etc. WN529, WN530, WN531, WN535, WN536, WN551, WN557 and NU516 up to 20260609. Affected by this issue is the function strcpy of the file upload.cgi of the component lighttpd. The manipulation of the argument HTTP_COOKIE leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2026-08-03	8.8	CVE-2026-18607

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wbolt.com--Spider Analyser-WordPress	Unauthenticated Remote Code Execution (RCE) in Spider Analyser; WordPress<= 2.1.3 versions.	2026-08-06	10	CVE-2026-65553
Weaver Network Co., Ltd.--E-cology 9.0	Weaver (Fanwei) E-cology 9.0 versions prior to 10.52 contain a file upload vulnerability that allows a remote, unauthenticated attacker to upload arbitrary files, including JSP webshells, by submitting a multipart/form-data POST request to /workrelate/plan/util/uploaderOperate.jsp with arbitrary secd and plandetailid field values. Successful exploitation results in remote code execution under the privileges of the application server process. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-14 (UTC).	2026-08-07	9.8	CVE-2022-4995
WebAppick--CTX Feed	Shop manager Remote Code Execution (RCE) in CTX Feed <= 6.6.42 versions.	2026-08-06	9.1	CVE-2026-66709
WebPros--Plesk	An SQL injection vulnerability in Plesk Obsidian up to 18.0.80 for Linux and Windows allows an authenticated user to read arbitrary data from the panel database.	2026-08-07	7.7	CVE-2026-64636
WebsiteBaker Org e.V.--WebsiteBaker CMS	WebsiteBaker CMS before 2.13.10 contains a code injection vulnerability in the Droplets editor that allows authenticated administrators to inject arbitrary PHP code by submitting malicious content through the droplet Code field, which is written verbatim to a publicly accessible PHP file with no content sanitization. Attackers can save a PHP webshell via the save_droplet handler to a predictable path inside the modules directory, enabling unauthenticated users to achieve remote code execution by making direct HTTP requests to the written file.	2026-08-03	7.2	CVE-2026-61523
WebsiteBaker Org e.V.--WebsiteBaker CMS	WebsiteBaker CMS before 2.13.10 contains an unrestricted file upload vulnerability in the module installation feature that allows authenticated administrators to achieve remote code execution by uploading a crafted ZIP archive containing a PHP webshell alongside a valid info.php metadata file. Attackers can place the malicious archive through the module installation interface, causing the application to extract the webshell into a web-accessible modules/ subdirectory where it becomes immediately executable by any unauthenticated user via direct HTTP request.	2026-08-03	7.2	CVE-2026-61524
wisemattic--wiseCampaign WooCommerce Conversions Made Easy	The wiseCampaign - WooCommerce Conversions Made Easy plugin for WordPress is vulnerable to unauthorized modification and disclosure of data due to every one of its REST API endpoints being registered with `permission_callback => '__return_true'` in all versions up to, and including, 1.1.16. This makes it possible for unauthenticated attackers to read and modify the plugin's banner, stockbar, and core settings - including saving/updating banner records, toggling stockbar/feature flags, changing the active banner, and uploading background-image files via wp_handle_upload() - without any nonce or capability check.	2026-08-05	7.5	CVE-2026-7529
wp-downloadmanager --wp-downloadmanager	The wp-downloadmanager WordPress plugin, in version 1.68.11 (also affecting the 6.9.4 release line), allows an admin-privileged user (current_user_can('manage_downloads')) to upload arbitrary files via download-add.php with no extension or MIME-type validation of any kind - no wp_check_filetype_and_ext(), no validate_file(), and no extension blacklist exist anywhere in the upload handler. The destination path is additionally built by concatenating the raw, unsanitized \$_POST['file_upload_to'] value with no traversal check (no ../ filtering, no basename()/realpath() applied). Since the base download path is required to live under WP_CONTENT_DIR (a web-accessible location), an uploaded PHP file lands in a web-servable path and can be directly executed, resulting in remote code execution. The plugin's own later changelog confirms these protections were absent in this version: v1.69 added file-type validation via wp_check_filetype_and_ext(), and v1.69.1 added directory-traversal protection - neither existed in 1.68.11.	2026-08-05	7.2	CVE-2026-18933
wp.insider--Simple Membership	Unauthenticated Broken Access Control in Simple Membership <= 4.7.8 versions.	2026-08-06	7.5	CVE-2026-66712
WPC Name Your Price for WooCommerce--WPC Name Your Price for WooCommerce	The WPC Name Your Price for WooCommerce WordPress plugin before 2.2.5 does not enforce its server-side price allowlist for products configured in "Select" price mode, allowing an unauthenticated visitor to add such a product to the cart at an arbitrary value below the merchant-defined allowed prices and commit a real order at that price (revenue loss / underpriced orders). This is a distinct, unfixed vector from CVE-2025-12115, whose 2.2.0 fix only addressed applying a custom price to products where Name Your Price is disabled and left the Select-mode allowlist unenforced through 2.2.4.	2026-08-06	7.5	CVE-2026-16620
wpDataTables--wpDataTables	Unauthenticated Cross Site Scripting (XSS) in wpDataTables <= 7.5.1 versions.	2026-08-06	7.1	CVE-2026-65509

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WPDeveloper--EmbedPress	Unauthenticated Cross Site Scripting (XSS) in EmbedPress <= 4.5.6 versions.	2026-08-06	7.1	CVE-2026-61961
wpdreams--Ajax Search Lite	Unauthenticated PHP Object Injection in Ajax Search Lite <= 4.14.4 versions.	2026-08-06	9.8	CVE-2026-28139
wpjobportal--WP Job Portal	Subscriber SQL Injection in WP Job Portal <= 2.5.6 versions.	2026-08-06	8.5	CVE-2026-65569
wpmanageninja--FluentSMTP WP SMTP Plugin with Amazon SES, SendGrid, Mailgun, Postmark, Cloudflare, toSend, Gmail and Any SMTP	The FluentSMTP - WP SMTP Plugin with Amazon SES, SendGrid, MailGun, Postmark, Google and Any SMTP Provider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Recipient Display Name (to.name) in Email Logs in all versions up to, and including, 2.2.95 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload is delivered via an attacker-controlled recipient display name (to.name) in a wp_mail() call and does not fire in the log list view - only in the detail view when an administrator uses the Prev/Next navigation controls, as that path bypasses the escapeHtml pipeline used by the list view.	2026-08-06	7.2	CVE-2026-16636
WPManageNinja--Ninja Tables	Unauthenticated Cross Site Scripting (XSS) in Ninja Tables <= 5.2.9 versions.	2026-08-06	7.1	CVE-2026-61964
WPMU DEV--Forminator	Contributor Privilege Escalation in Forminator <= 1.56.0 versions.	2026-08-06	8.8	CVE-2026-28111
WPMU DEV--Forminator	Unauthenticated Cross Site Scripting (XSS) in Forminator <= 1.56.0 versions.	2026-08-06	7.1	CVE-2026-28143
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Forged Upload Record via Select Field in all versions up to, and including, 1.56.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit is possible because Forminator_Core::sanitize_array() skips all filtering for keys prefixed with 'select-', and set_field_data() treats a submitted 'return' member as a trusted internal flag - allowing an unauthenticated attacker to forge and persist a complete upload field record with an arbitrary file_url value without any sanitization or validation.	2026-08-06	7.2	CVE-2026-18325
wpmudev--WPMU DEV Dashboard	The WPMU DEV Dashboard plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 5.0.0. On sites not yet connected to the WPMU DEV Hub - the default state after installation - the site API key that keys the WDP-AUTH request signature is empty, making the signature verified by validate_hash() trivially forgeable; version 5.0.0 additionally removed the replay check in validate_nonce(), and the remote handler is bound to the public init hook with no capability check. This makes it possible for unauthenticated attackers to invoke privileged Hub actions - including installing and activating a plugin from an attacker-supplied URL (resulting in remote code execution), deleting plugins and themes, upgrading WordPress core, or logging in as an administrator via SSO. Sites connected to a WPMU DEV account, which have a non-empty 64-character API key, are not affected.	2026-08-06	8.1	CVE-2026-15459
wpwax--FormGent Next-Gen AI Form Builder for WordPress with Multi-Step, Quizzes, Payments & More	The FormGent - Next-Gen AI Form Builder for WordPress with Multi-Step, Quizzes, Payments & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via form submission fields in all versions up to, and including, 1.9.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-06	7.2	CVE-2025-15028
WSO2--WSO2 API Manager	In multi-tenant deployments, the Publisher REST APIs fail to enforce tenant isolation correctly. This allows a user in one tenant, possessing sufficient privileges to invoke these APIs, to perform operations that impact other tenants. The vulnerability allows a privileged user to perform publisher operations such as exposing or modifying API Metadata in another tenant environment. This impact is only realized in multi-tenant deployments.	2026-08-06	9	CVE-2025-14561
WSO2--WSO2 API Manager	Tokens issued to a low-privileged user are not sufficiently restricted, allowing them to be used to access product-level Admin REST APIs. Exploitation of this vulnerability allows a low-privileged user to invoke the Admin REST APIs of WSO2 products, potentially leading to full administrative account takeover. This requires the attacker to already possess a low-privileged user account and be able to obtain a valid token for it.	2026-08-06	9.8	CVE-2026-1728

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WSO2--WSO2 API Manager	The System REST API accepts user-supplied file uploads without enforcing sufficient validation on the file type or destination, allowing files to be written to arbitrary server-accessible locations. Exploitation requires authenticated administrative access with publisher privileges. Successful exploitation permits an authenticated publisher to upload files to server-accessible locations. Depending on the deployment environment and how uploaded files are handled, this could lead to the execution of uploaded content, potentially resulting in remote code execution.	2026-08-06	9.1	CVE-2026-3418
WSO2--WSO2 API Manager	The XML and schema validation functionalities within the SchemaValidator Mediator process XML input as part of validation flows. Under certain conditions, the XML parser allows the resolution of external entities when handling user-supplied XML content during validation operations. This behavior can occur when an attacker supplies crafted XML payloads to the relevant mediator flows with sufficient privileges. Successful exploitation may allow a highly privileged actor to read files accessible within the server hosting the affected product. Additionally, it may be possible to trigger outbound requests to unintended internal or external locations, depending on the server environment and network configuration. Specially crafted XML payloads can also lead to excessive resource consumption during parsing, impacting the availability of the product.	2026-08-06	8.7	CVE-2026-3415
WSO2--WSO2 Identity Server	The Conditional Authentication (Adaptive Authentication) script does not correctly enforce the completion of all required authentication steps when a specific multi-step pattern involving certain authenticators is configured. This allows an attacker to bypass intermediate authentication challenges by exploiting how the script handles callbacks and re-execution of authentication steps. Successful exploitation allows a malicious actor to gain unauthorized access to a targeted user account. This vulnerability can only be exploited when all of the following conditions are met: the application login flow contains a specific secondary authenticator, the Conditional Authentication script is configured with particular event callbacks and re-executes an authentication step, the targeted user has one of the impacted authenticators enrolled, and the attacker successfully completes any preceding authentication steps.	2026-08-06	9.4	CVE-2025-15039
WSO2--WSO2 Universal Gateway	The JWT authentication mechanism accepts tokens signed with algorithms other than those explicitly configured or supported. This allows an attacker to craft a JWT with an unsupported algorithm, which is then incorrectly validated, leading to unauthorized access. Successful exploitation of this vulnerability may result in unauthorized access to the system, including the potential compromise of administrative accounts and full account takeover. The CVSS score is adjusted to 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) in single-tenant deployments, reflecting that the impact is contained within a single security authority boundary.	2026-08-06	10	CVE-2026-5430
wupsales--AI Copilot Content Generator	The AI Copilot - Content Generator plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.5.6. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to create a new administrator-level user account and achieve full site takeover by saving and executing a malicious workflow containing a wp_create_user action node specifying role=administrator. This vulnerability is exploitable by unauthenticated attackers on any site where the [aiwu-form] shortcode or public chatbot is rendered on a frontend page, as the waic-nonce value is emitted into publicly accessible JavaScript (WAIC_DATA.waicNonce) on those pages, rendering the nonce check a non-functional authorization barrier.	2026-08-08	9.8	CVE-2026-14526
wupsales--AI Copilot Content Generator	The AI Chatbot & Workflow Automation by AIWU plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.6. This is due to the `getCurrentTaskResults()` method in `modules/workspace/controller.php` being accessible without authentication or authorization checks. The method is not included in the workspace controller's `getNoncedMethods()` array, the base `getPermissions()` returns an empty array, and all AJAX actions are registered with `wp_ajax_nopriv_` hooks (`classes/frame.php:282`). When tasks are created via features like the Bulk Post Generator, the task parameters - including the OpenAI API key in plaintext, AI prompts, keywords, and full AI model configuration - are stored in the database and returned in the JSON response. This makes it possible for unauthenticated attackers to enumerate sequential task IDs and retrieve sensitive configuration data including API keys.	2026-08-05	7.5	CVE-2026-6639

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
XplodedThemes--WPIDE File Manager & Code Editor	Unauthenticated Cross Site Scripting (XSS) in WPIDE - File Manager & Code Editor <= 3.5.7 versions.	2026-08-06	7.1	CVE-2026-66440
Zbtlink--CPE2801 Firmware	Zbtlink router firmware ships an embedded remote-control implant, ENDLESSDOORS, present in every published build across the product line. It is the open-source ycsunjane/rctl tool built in as an OpenWrt package (librctl.so), started at boot and run as root under the process name kworker to blend in with the kernel's [kworker/*] threads. It opens no listening port; it phones home over cleartext TCP to a hardcoded command-and-control server (command channel 7000, interactive-shell callback 7001) with no authentication and no transport encryption, re-attempting contact roughly every 35 seconds. Its command handler passes any received string to popen() as uid=0, and a reserved rctlbash command returns an interactive root shell. Because the channel is unauthenticated and cleartext, control is not limited to whoever planted it: any party that answers at the C2 address, occupies the network path (DNS or route hijack), or acquires the hardcoded fallback domain obtains unauthenticated remote code execution as root.	2026-08-05	9.8	CVE-2026-66747
ZenML--ZenML	ZenML 0.94.6 contains a remote code execution vulnerability in the CloudpickleMaterializer component that allows attackers with write access to a shared artifact store to execute arbitrary code by planting a malicious pickle file. Attackers can replace a stored artifact.pkl file with a crafted cloudpickle payload containing a malicious __reduce__ method, which executes arbitrary system commands when any user or pipeline materializes the artifact through the unsanitized cloudpickle.load() call in cloudpickle_materializer.py.	2026-08-07	8	CVE-2026-68772
zephyrproject--zephyr	The hawkBit device management client in subsys/mgmt/hawkbit accumulates the body of an HTTP response from the update server into a heap buffer in response_json_cb() (subsys/mgmt/hawkbit/hawkbit.c). The buffer is sized to hold the received body bytes but reserves no space for a terminating NUL. When the full response has arrived, the code writes response_data[downloaded_size] = '\0' - and whenever the accumulated body length equals the allocation, that terminator lands one byte past the end of the heap object (a heap-based out-of-bounds write, CWE-122 / CWE-787). The body length and fragmentation are taken directly from the parsed HTTP response (rsp->body_frag_start / rsp->body_frag_len) and are fully controlled by the remote hawkBit server, which chooses its own response length. The precise trigger depends on how the buffer grows, and both forms are remotely reachable. Since v4.0.0 the reallocation is sized to exactly downloaded_size + body_len, so any response body larger than the 1100-byte initial buffer makes the out-of-bounds write deterministic; such response sizes are normal for hawkBit deployment metadata. Before v4.0.0 the buffer grew by doubling and the growth check ((downloaded_size + body_len) > response_buffer_size) is false at equality, so a response body whose length is exactly the current allocation - 1100 bytes with the default initial buffer - skips the reallocation entirely and writes the terminator at response_data[1100] of an 1100-byte object. The HTTP length-mismatch check does not catch this, because the declared and received lengths genuinely agree. Either form is reachable by a malicious, compromised, or man-in-the-middle update server (TLS is optional and, when enabled, does not protect against a hostile server), with no authentication of response content and no client-side length cap protecting the write. The out-of-bounds write is a fixed single NUL byte immediately following the allocation, corrupting adjacent allocator metadata or the next allocation. The practical impact is heap corruption leading to denial of service (fault on a subsequent allocation or free), with the bounded, allocator-dependent possibility of further corruption. The fix sizes the buffer to the body length plus one and copies with memcpy, ensuring the terminator always lands within the allocation.	2026-08-03	8.2	CVE-2026-10849
zephyrproject--zephyr	The Bluetooth host ATT layer (subsys/bluetooth/host/att.c) associates each in-flight ATT TX buffer with its owning channel via the static tx_meta_data_storage[] array (data->att_chan = chan). When a buffer's last reference is dropped, its netbuf destroy callback defers the completion handling to the system workqueue (att_tx_destroy -> att_tx_destroy_work_handler -> att_on_sent_cb -> bt_att_sent), where bt_att_sent dereferences the channel and its ATT context (sys_slist_get(&att->reqs)). When a peer disconnects while an ATT PDU (a server notification/indication or any response) is still in flight in the controller TX path, L2CAP tears the channel down in l2cap_chan_del(): it runs the disconnected callback and then the released callback (bt_att_released), which frees the channel	2026-08-04	7.1	CVE-2026-11368

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	slab slot. Because the in-flight buffer is held by the connection TX path rather than the channel's own queue, its deferred destroy work can run after the channel has been freed. The att_on_sent_cb guard intended to drop the stale callback itself dereferences meta->att_chan, which is now a dangling pointer into a freed (and possibly reused) slab slot. A remote peer with an ATT connection can drive this by disconnecting during routine ATT traffic; no pairing or user interaction is required to reach the ATT bearer. The result is a use-after-free read/write of freed channel memory, reliably crashing the Bluetooth host (denial of service) and, because the channel slab slot may be reused, potentially corrupting live memory. The fix makes bt_att_released() NULL the att_chan field of every tx_meta_data_storage[] entry still referencing the channel before freeing it, so the deferred guard observes a NULL pointer and drops the callback. Teardown and the destroy work both run on the cooperative system workqueue, so the array update is serialized and needs no lock.			
ZTE--F689	By accessing unencrypted information in the device firmware, an attacker can obtain the initial login credentials for the device's web interface.	2026-08-07	7.5	CVE-2026-49007
Zucchetti S.p.a.--FirmaCheck	FirmaCheck for Windows before 1.3.16 contains a DLL hijacking vulnerability that allows local attackers to execute arbitrary code by placing a crafted openssl.cnf file in the unvalidated C:\Program Files (x86)\Common Files\SSL\ directory path. Attackers can write a malicious OpenSSL configuration file referencing an attacker-controlled DLL to achieve code execution at startup process privilege level when FirmaCheck.exe runs automatically at system startup.	2026-08-03	7.8	CVE-2026-41447
Zyxel--ATP series firmware	A path traversal vulnerability in the CLI command used to execute configuration files in Zyxel ATP series firmware versions from V4.32 through V5.42 Patch 1, USG FLEX series firmware versions from V4.50 through V5.42 Patch 1, USG FLEX 50(W) series firmware versions from V4.16 through V5.42 Patch 1, and USG20(W)-VPN series firmware versions from V4.16 through V5.42 Patch 1 could allow an authenticated attacker with administrator privileges to execute a crafted malicious configuration file on an affected device.	2026-08-04	7.2	CVE-2026-14818
Zyxel--WAX650S firmware	A post-authentication command injection vulnerability in the "export-cgi" CGI program in Zyxel WAX650S firmware versions through 7.10(ABRM.4)C0 could allow an authenticated attacker with administrator privileges to execute OS commands on an affected device.	2026-08-04	7.2	CVE-2026-6837
1meril--Blog Floating Button	Unauthenticated Cross Site Scripting (XSS) in Blog Floating Button <= 1.4.20 versions.	2026-08-13	7.1	CVE-2026-28170
4xmen--pm2panel	An OS command injection vulnerability in 4xmen/pm2panel (all versions) allows an authenticated remote attacker to execute arbitrary system commands on the host. The pm2panel.js handler at line 188 passes the unsanitized req.query.id parameter directly to exec('pm2 restart ' + id) without input validation or shell escaping, enabling command chaining via semicolons or other shell metacharacters.	2026-08-10	8.8	CVE-2026-72573
@fastify/busboy--@fastify/busboy	@fastify/busboy is a multipart form-data parser. In versions 1.0.0 through 3.2.0, an attacker who can submit multipart form-data can crash the parser by sending a part header whose name is a prototype-inherited property such as __proto__ or constructor. The internal header parser stores headers in a plain JavaScript object and assumes each value is an array, so an inherited property name resolves to a truthy non-array value and triggers a TypeError. In the common pipe integration the failure surfaces as an error event, but in direct write or end usage the exception is thrown synchronously and can terminate the Node.js process, causing an unauthenticated denial of service. The issue is fixed in @fastify/busboy 3.2.1, which creates the header object with a null prototype. Users should upgrade to 3.2.1.	2026-08-13	7.5	CVE-2026-19481
@fastify/busboy--@fastify/busboy	@fastify/busboy is a multipart form-data parser. In versions 3.1.0 through 3.2.0, a remote unauthenticated attacker can stall the Node.js event loop by sending a multipart request whose boundary is crafted to a specific length. The vendored streaming search stores its skip table in a fixed 256 entry byte array, and a boundary of exactly 252 bytes makes the search needle 256 bytes, which truncates the default skip distance to zero and turns the search into a CPU bound loop on a small body. A single small request can keep one core busy and deny service to other requests handled by the same process. The issue is fixed in @fastify/busboy 3.2.1, which widens the skip table so the skip distance is preserved. Users should upgrade to 3.2.1.	2026-08-13	7.5	CVE-2026-19484
@fastify/jwt--@fastify/jwt	@fastify/jwt is a JSON Web Token plugin for Fastify. In versions before 10.2.2, a per-request verification key passed to request.jwtVerify({ key }) is silently overridden by the plugin's globally configured secret, because the option merge	2026-08-15	8.1	CVE-2026-18500

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	applies the global key last. Applications that use different keys for different authorization domains, for example separate user and admin keys, therefore accept a token signed with the global key on a route that explicitly requires another key. This lets an ordinary authenticated user cross a key-based trust boundary without knowing either secret. The issue is fixed in @fastify/jwt 10.2.2, where an explicit per-call key takes precedence over the global secret. Users should upgrade to 10.2.2.			
@fastify/multipart -- @fastify/multipart	@fastify/multipart is a multipart form-data parser for Fastify. In versions from 5.3.0 up to but not including 10.1.1, when the busboy fileSize limit truncates a file part, the plugin clears its internal current-file reference while the underlying stream is still open. If the client then aborts the connection before sending the terminating boundary, the abort cleanup finds no stream to destroy, so saveRequestFiles() never settles, the request handler hangs, and the temporary file already written to disk is never cleaned up. An unauthenticated client can repeat this to permanently leak temporary files and suspended handler executions, leading to disk and event-loop exhaustion. The issue is fixed in @fastify/multipart 10.1.1. Users should upgrade to 10.1.1.	2026-08-15	7.5	CVE-2026-18549
@fastify/multipart -- @fastify/multipart	@fastify/multipart is a multipart form-data parser for Fastify. In versions from 3.0.0 up to but not including 10.1.1, request.saveRequestFiles() can leave completed temporary files on disk when a client disconnects while the parser is advancing between multipart parts. The iterator rejection that occurs between parts falls outside the per-file cleanup path, so an earlier completed file is never removed. An unauthenticated client can repeat this to cause persistent, linear disk consumption, leading to denial of service. This is an incomplete-fix variant of CVE-2025-24033. The issue is fixed in @fastify/multipart 10.1.1. Users should upgrade to 10.1.1.	2026-08-15	7.5	CVE-2026-19474
acyba--AcyMailing An Ultimate Newsletter Plugin and Marketing Automation Solution for WordPress	The AcyMailing - An Ultimate Newsletter Plugin and Marketing Automation Solution for WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 10.11.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to overwrite the BCC field of the acy_notification_cms notification template, causing subsequent WordPress password-reset emails - including those targeting administrator accounts - to be silently copied to an attacker-controlled address, enabling account takeover via the captured reset link. Successful exploitation requires the site administrator to have enabled the "Send website emails with AcyMailing" option, which routes WordPress core notification emails through AcyMailing's templating system.	2026-08-11	8.8	CVE-2026-15426
Admidio--admidio	Admidio is an open-source user management solution. Prior to version 5.0.10, `modules/documents-files.php` gates state-changing modes by checking that the actor has `hasUploadRight()` on the URL parameter `folder_uuid`. The `move_save` handler then operates on a *separate* URL parameter `file_uuid` and calls `File::moveToFolder(\$destFolderUUID)`. `File::moveToFolder()` checks the upload right on the destination folder but never on the source folder containing the file. As a result, any user who can upload to any single folder can move any file from any other folder - including private folders to which they have no view rights - into a folder they control, and then download it. Confidentiality is broken (private file contents leak) and integrity is broken (the file is removed from the original location). Version 5.0.10 contains a fix.	2026-08-12	8.1	CVE-2026-47231
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-11	10	CVE-2026-27302
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-11	10	CVE-2026-71398
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-11	9	CVE-2026-48381
Adobe--Adobe Commerce	Adobe Commerce is affected by an Incorrect Authorization vulnerability that could result in privilege escalation. An attacker could leverage this vulnerability to gain	2026-08-11	9.1	CVE-2026-71362

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	elevated access to sensitive resources. Exploitation of this issue does not require user interaction.			
Adobe--Adobe Commerce	Adobe Commerce is affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, potentially gaining elevated access or control over the victim's account or session. Scope is changed.	2026-08-11	8.7	CVE-2026-48413
Adobe--Adobe Commerce	Adobe Commerce is affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, potentially gaining elevated access or control over the victim's account or session. Exploit depends on conditions beyond the attacker's control. Scope is changed.	2026-08-11	7.7	CVE-2026-48414
Adobe--Adobe Commerce	Adobe Commerce is affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access, causing a limited disruption to availability. Exploitation of this issue does not require user interaction.	2026-08-11	7.6	CVE-2026-48415
Adobe--Adobe Commerce	Adobe Commerce is affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction.	2026-08-11	7.5	CVE-2026-48416
Adobe--ColdFusion 2025	ColdFusion is affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-11	10	CVE-2026-48362
Adobe--ColdFusion 2025	is affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access, potentially resulting in an application denial-of-service condition. The vulnerable component is restricted to an administrative network zone by default. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-11	9.6	CVE-2026-71384
Adobe--ColdFusion 2025	is affected by an Improper Input Validation vulnerability that could result in privilege escalation. A low-privileged attacker could exploit this vulnerability to gain unauthorized read and write access. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-08-11	8.7	CVE-2026-21273
Adobe--ColdFusion 2025	is affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and limited write access. Exploitation of this issue does not require user interaction.	2026-08-11	8.2	CVE-2026-21279
Adobe--ColdFusion 2025	is affected by a Use of Hard-coded Cryptographic Key vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-11	8.4	CVE-2026-34635
Adobe--ColdFusion 2025	ColdFusion is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction.	2026-08-11	8.1	CVE-2026-48440
Adobe--ColdFusion 2025	is affected by a Cross-site Scripting (XSS) vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. The vulnerable component is restricted to an administrative network zone by default. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-08-11	8.8	CVE-2026-71386
Adobe--ColdFusion 2025	ColdFusion is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. The vulnerable component is restricted to an administrative network zone by default. Exploitation of this issue does not require user interaction.	2026-08-11	8.8	CVE-2026-71387
Adobe--ColdFusion 2025	is affected by an Incorrect Authorization vulnerability that could result in privilege escalation. A low-privileged attacker could exploit this vulnerability to gain unauthorized read and write access. Exploitation of this issue does not require user interaction.	2026-08-11	7.8	CVE-2026-25652

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--ColdFusion 2025	ColdFusion is affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-11	7.7	CVE-2026-48385
Adobe--ColdFusion 2025	ColdFusion is affected by a Use of a Broken or Risky Cryptographic Algorithm vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue does not require user interaction.	2026-08-11	7.5	CVE-2026-48386
Adobe--ColdFusion 2025	is affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain limited unauthorized read and write access, causing a limited disruption to availability. Exploitation of this issue does not require user interaction.	2026-08-11	7.3	CVE-2026-71383
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	7.5	CVE-2026-48438
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	7.5	CVE-2026-48439
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a Arbitrary file system read. An attacker could leverage this vulnerability to gain unauthorized read access to files or directories outside the intended restrictions. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-11	7.1	CVE-2026-48442
Adobe--Lightroom Classic	Lightroom Classic is affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-08-11	8.6	CVE-2026-48397
Adobe--Lightroom Classic	Lightroom Classic is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-08-11	8.6	CVE-2026-48441
Adobe--Lightroom Classic	Lightroom Classic is affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-11	7.8	CVE-2026-47940
Adobe--Lightroom Classic	Lightroom Classic is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-11	7.8	CVE-2026-48404
Adobe--Lightroom Classic	Lightroom Classic is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-11	7.8	CVE-2026-48405
Adobe--Lightroom Classic	Lightroom Classic is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-11	7.8	CVE-2026-48406
Adobe--Lightroom Classic	Lightroom Classic is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-11	7.8	CVE-2026-48407
Adobe--Lightroom Classic	Lightroom Classic is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-11	7.8	CVE-2026-48408
Adobe--Lightroom Classic	Lightroom Classic is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-11	7.8	CVE-2026-48409
Adobe--Lightroom Classic	Lightroom Classic is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-11	7.8	CVE-2026-48410

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Lightroom Classic	Lightroom Classic is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-08-11	7.7	CVE-2026-48447
Afonso Matos--Arvow AI SEO Writer	Unauthenticated Broken Access Control in Arvow AI SEO Writer <= 1.5.3 versions.	2026-08-13	7.5	CVE-2026-66469
AgniHD--Cartify	Unauthenticated Broken Authentication in Cartify <= 1.3.0.1 versions.	2026-08-13	9.8	CVE-2026-66465
ahmadgb--GeekyBot	Unauthenticated Cross Site Scripting (XSS) in GeekyBot <= 1.2.6 versions.	2026-08-13	7.1	CVE-2026-61965
ai--nanoid	nanoid is a secure, URL-friendly, unique string ID generator for JavaScript. Prior to versions 3.3.12 and 5.1.11, the nanoid(size) function in index.js and index.cjs coerces the user-influenced size parameter to a signed 32-bit integer, allowing a value of 2147483648 to become -2147483648 and corrupt the process-wide CSPRNG poolOffset in fillPool(), which causes subsequent session tokens, CSRF tokens, API keys, and unique identifiers to become the deterministic string "aaaaaaaaaaaaaaaaaaaa" until the process restarts. This issue is fixed in versions 3.3.12 and 5.1.11.	2026-08-11	7.4	CVE-2026-73086
alldatacenter--alldata	A vulnerability was detected in alldatacenter alldata up to 0.6.8. This affects the function Hessian2Input.readObject of the file /serialize/impl/HessianSerializer.java of the component xxi-rpc Listener. The manipulation results in deserialization. The attack may be performed from remote. The exploit is now public and may be used. The project closed the issue report as "not planned" without any further explanation.	2026-08-14	7.3	CVE-2026-19826
alseambusher--crontab-ui	An OS command injection vulnerability in alseambusher/crontab-ui through 0.4.2 allows an unauthenticated remote attacker to execute arbitrary system commands by importing a crafted crontab database file. The POST /import endpoint accepts arbitrary .db files and overwrites the application database without validation.	2026-08-10	9.8	CVE-2026-72589
alseambusher--crontab-ui	An OS command injection vulnerability in alseambusher/crontab-ui through 0.4.2 allows an unauthenticated remote attacker to inject arbitrary cron job entries by sending a crafted GET request to /crontab with URL-encoded newlines in the env_vars parameter.	2026-08-10	9.8	CVE-2026-72590
Amauri--WPMobile.App	Unauthenticated Broken Access Control in WPMobile.App <= 11.77 versions.	2026-08-13	7.5	CVE-2026-61984
andy_moyle--Church Admin	Unauthenticated SQL Injection in Church Admin <= 5.1.1 versions.	2026-08-13	9.3	CVE-2026-66478
anephenix--hub	Hub is a Node.js WebSocket server and client with added features. Prior to 0.2.16, every incoming unauthenticated WebSocket connection triggers loadDefaultConnectionEventListeners to call requestClientId, which calls rpc.send for the get-client-id action and pushes a request into RPC.requests. The RPC.waitForReply function starts a setInterval polling loop every 10 milliseconds that is cleared only after a matching reply; if the client remains silent and closes, the timer and pending request stay allocated because the socket close path does not cancel them. Repeated connections therefore cause unbounded timers and heap entries, exhausting CPU and memory and making the server unavailable. This issue is fixed in version 0.2.16.	2026-08-13	7.5	CVE-2026-73561
Aonetheme--Service Finder Booking	Subscriber Privilege Escalation in Service Finder Booking <= 6.2 versions.	2026-08-13	8.8	CVE-2026-28161
Apioo--Fusio	A remote code execution vulnerability in Apioo Fusio 8.8.3 allows authenticated users with the Developer role to execute arbitrary OS commands by exploiting a PHP-Sandbox allow-list bypass. The sandbox allow-list permits functions that transitively invoke system(), enabling a developer to escape the sandbox and gain OS command execution on the server. An attacker with a Developer-role account can achieve full server compromise.	2026-08-11	8.8	CVE-2026-72551
Arcadia Technology, LLC--Crafty Controller	Path traversal in server import and admin file upload in Crafty Controller. Allows a remote, authenticated attacker to upload files to arbitrary paths permitted to the Crafty Controller application and perform remote code execution.	2026-08-11	9.1	CVE-2026-13716
Arraytics--Booktics	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Arraytics Booktics allows Blind SQL Injection. This issue affects Booktics: from n/a through 1.0.22.	2026-08-13	8.5	CVE-2026-28002
Arraytics--WP Event SOLUTION	Customer Arbitrary Content Deletion in WP Event SOLUTION <= 4.1.19 versions.	2026-08-13	7.1	CVE-2026-28173

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ASP-CMS Project-- ASP-CMS	ASP-CMS contains a SQL injection vulnerability in the commentList.asp endpoint that allows unauthenticated remote attackers to inject arbitrary SQL by manipulating the id parameter in GET requests to the comment listing script. Attackers can bypass the application's keyword blocklist by interleaving the string 'master' within blocked SQL terms to extract sensitive database contents. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-18 (UTC).	2026-08-13	7.5	CVE-2019-25765
AsyncFuncAI-- deepwiki-open	An improper path validation vulnerability in AsyncFuncAI/deepwiki-open through commit 16f35a0 allows unauthenticated remote attackers to write to or delete arbitrary files with root privileges. The api/api.py wiki-cache endpoint constructs file paths from user-controlled owner, repo, and repo_type fields without sanitization, enabling path traversal.	2026-08-10	9.8	CVE-2026-72567
AsyncFuncAI-- deepwiki-open	A path traversal vulnerability in AsyncFuncAI deepwiki-open through commit 16f35a0 allows unauthenticated remote attackers to obtain directory listings for arbitrary filesystem paths via the local-repository structure endpoint. The endpoint accepts an absolute filesystem path parameter and returns a directory listing without authentication, as WIKI_AUTH_MODE defaults to false. An attacker can enumerate sensitive directory contents on the host system.	2026-08-11	7.5	CVE-2026-72602
Attendize-- Attendize	An insecure direct object reference vulnerability in Attendize through commit 9289acb allows any authenticated event organiser to inject attendees and orders into events belonging to other accounts via the postInviteAttendee endpoint. The endpoint loads the target event by ID without scoping the query to the authenticated organiser account. An attacker can modify event data and financial records across account boundaries.	2026-08-11	7.1	CVE-2026-72546
Attendize-- Attendize	An insecure direct object reference vulnerability in Attendize through commit 9289acb allows any authenticated event organiser to bulk import attendees into events belonging to other accounts via the postImportAttendee endpoint. The endpoint loads the target event by ID without verifying ownership against the requesting organiser account. An attacker can inject bulk attendee data into any event in the system regardless of account boundaries.	2026-08-11	7.1	CVE-2026-72547
Authentik Security-- -authentik	A privilege escalation vulnerability in Authentik Security authentik through 2026.5.6 allows an attacker with a source-scoped SCIM provisioning token to gain superuser privileges by provisioning a SCIM group that matches an existing administrator group by name. The SCIM group ingest function adopts any existing group by name and replaces its membership without validating the source scope against the target group. An attacker can grant their provisioning token full IdP superuser access and lock out all existing administrators.	2026-08-11	8.8	CVE-2026-72534
Authentik Security-- -authentik	A privilege escalation vulnerability in Authentik Security authentik through 2026.5.6 allows an attacker with a source-scoped SCIM provisioning token to take over any user account including superusers by provisioning a SCIM user that matches an existing local user by username. The SCIM user ingest function adopts pre-existing local accounts by username without validating scope boundaries. An attacker can rewrite or delete any account, including the superuser, using only a limited provisioning credential.	2026-08-11	8.8	CVE-2026-72537
Autodesk--Installer	A maliciously created executable, when executed on the victim's machine, may allow a local low-privileged attacker to inject unauthenticated IPC messages into named pipes, modify pipe permissions or ownership, and potentially impact confidentiality, integrity, and availability.	2026-08-12	7.8	CVE-2026-14478
automatisch-- automatisch	A server-side request forgery (SSRF) vulnerability in automatisch through commit 41f3c56 allows a low-privileged authenticated user with 'manage Flow' permission to make the server fetch arbitrary URLs and retrieve the full response body via the HTTP Request app's Custom Request action.	2026-08-10	7.7	CVE-2026-72566
AWS--OpenSearch	Missing authorization in the Execute Monitor API in Amazon OpenSearch Alerting plugin might allow an authenticated remote user to read, modify, or delete arbitrary index data via a crafted inline monitor request with unintentional data source and input index parameters.	2026-08-12	8.1	CVE-2026-19311
AWS--Opensearch	A SQL query validation bypass in the Flint extension query handler in the OpenSearch SQL plugin allows a remote authenticated actor with async query access to execute arbitrary code on Apache Spark workers by sending a crafted SQL query to the direct query endpoint.	2026-08-13	8.8	CVE-2026-18428
AWS--Opensearch	Missing input validation in the threat intelligence feed parser in the OpenSearch Security Analytics plugin might allow an authenticated remote user to perform server-side request forgery and read local files via a crafted URL parameter to the threat intel source configuration endpoint.	2026-08-12	8.1	CVE-2026-18952

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Axis Communications AB--AXIS OS	A VAPIX API parameter had improper input validation which could allow code execution and potentially lead to a privilege escalation. This flaw can only be exploited after authenticating with an administrator-privileged service account.	2026-08-11	7.2	CVE-2026-4757
BadChoice--Handesk	A broken access control vulnerability in BadChoice Handesk as of 2026-07-10 allows any authenticated agent to overwrite lead records belonging to other teams via the LeadsController@update endpoint. The endpoint performs no authorization check, and the Lead model has guarded set to an empty array making all columns mass-assignable. An attacker with any agent account can corrupt lead data across team boundaries.	2026-08-11	8.1	CVE-2026-72563
BadChoice--Handesk	A broken access control vulnerability in BadChoice Handesk as of 2026-07-10 allows any authenticated agent to update ticket records belonging to other teams via the TicketsController@update endpoint. The endpoint calls no authorize() method and performs no team-scoped ownership check. An attacker with any agent account can modify, escalate, or corrupt tickets assigned to other teams.	2026-08-11	8.1	CVE-2026-72595
Baicells--EG3661M	A vulnerability was identified in Baicells EG3661M BaiCE_BQ6_2.0.5.3_NA. This impacts an unknown function of the file /cgi-bin/luci of the component LuCI Web Interface. Such manipulation of the argument MaxHops/Timeout/Size leads to os command injection. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-14	7.2	CVE-2026-19771
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Version 3.16.1 has a CSV injection vulnerability in the result export functionality. The application does not sanitize or escape user-supplied input when generating CSV files. An attacker can inject spreadsheet formulas into input fields, which are later executed when an administrator opens the exported CSV in spreadsheet software such as Microsoft Excel or LibreOffice Calc. Version 3.17.0 patches the issue.	2026-08-11	9.6	CVE-2026-47705
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Versions prior to 3.17.0 allow a low-privilege read collaborator to extract a workspace OAuth `credentialsId` from a readable bot configuration and then overwrite that credential through `handleUpdateOAuthCredentials()` by supplying an attacker-controlled writable `workspaceId`. The update path validates only the attacker-supplied workspace and then updates the credential record by global `id` alone, while also rewriting the credential's `workspaceId`. This allows cross-workspace OAuth credential takeover and reassignment. Version 3.17.0 patches the issue.	2026-08-11	9.9	CVE-2026-48765
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Versions prior to 3.17.0 expose a deprecated public upload endpoint at `GET /api/v1/typebots/{typebotId}/blocks/{blockId}/storage/upload-url` that accepts an attacker-controlled `filePath` and returns a presigned S3 `PUT` URL for that exact key. Because the endpoint only checks that the referenced typebot is public and that the referenced block is a file input block, an unauthenticated attacker who knows a valid public `typebotId` and `blockId` can request presigned upload URLs for arbitrary objects in the shared bucket, including `private/...` and other tenants' `public/...` paths. Version 3.17.0 fixes this issue.	2026-08-11	8.2	CVE-2026-48763
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Prior to version 3.17.0, the `handleGetSheets` API handler (`POST /api/sheets/getSheets`) does not validate workspace membership, allowing any authenticated user to access and decrypt another workspace's Google Sheets OAuth credentials and retrieve spreadsheet data (sheet names, IDs, column headers). Version 3.17.0 fixes the issue.	2026-08-11	7.1	CVE-2026-42142
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Prior to version 3.17.0, the Google Sheets OAuth callback decodes a base64-encoded JSON `state` parameter and trusts the embedded `workspaceId`, `typebotId`, `blockId`, and `redirectUrl` without cryptographic integrity protection or authorization checks. The callback route is authenticated, but it does not verify that the authenticated user has write access to the target workspace or Typebot before creating credentials in the workspace or updating Typebot groups. An authenticated user who can obtain a valid Google OAuth `code` can alter the `state` value to create Google Sheets credentials in another workspace and, if target IDs are known, attach those credentials to a block in another Typebot. Version 3.17.0 patches the issue.	2026-08-11	7.1	CVE-2026-48495
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Versions prior to 3.17.0 allow a low-privilege guest member of a workspace to exfiltrate stored OpenAI-compatible API keys by invoking the OpenAI model-listing helper with an attacker-controlled `baseUrl`. The vulnerable path decrypts the selected workspace credential, creates an OpenAI client with the secret in both `apiKey` and the explicit `api-key` header, and then sends the outbound request to the caller-supplied URL. Because the permission	2026-08-11	7.6	CVE-2026-48766

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	check accepts any readable workspace member and `listCredentials` reveals credential identifiers to guests, a guest can force the server to deliver the workspace secret to attacker infrastructure. Version 3.17.0 patches the issue.			
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Versions prior to 3.17.0 allow a low-privilege guest member of a workspace to obtain a live Google Sheets OAuth access token for that workspace by calling the Google Sheets helper `getAccessToken`. The vulnerable path checks only whether the caller has read access to the workspace, decrypts the stored Google OAuth credential, refreshes or retrieves the access token through the Google client, and returns the raw bearer token directly to the caller. Because guest members can also enumerate credential identifiers, a guest can mint and reuse the workspace's Google access token outside Typebot. Version 3.17.0 patches the issue.	2026-08-11	7.6	CVE-2026-48767
benoitc--erlang_quic	erlang_quic is a pure Erlang QUIC implementation. Prior to version 1.4.4, the QUIC client did not authenticate the server during the TLS 1.3 handshake. The CertificateVerify signature was not checked, the certificate chain was not validated, and the hostname was not compared against the certificate, so `verify` was effectively a no-op on the client. A man-in-the-middle on the network path could present any certificate and impersonate any server, defeating the confidentiality and integrity of the connection. HTTP/3 uses the same client and was equally affected. Handshakes authenticated by a PSK (session resumption) are not affected, because the peer is authenticated by the PSK binder and no certificate is sent. This is fixed in 1.4.4. The client now verifies the CertificateVerify signature, validates the certificate chain against the trust store (`cacerts` option, the operating system store by default), and checks the hostname. Client `verify` now defaults to on; set `verify => false` to accept any certificate (for example a self-signed test server). No known workarounds are available before 1.4.4. `verify => true` had no effect, and inspecting the certificate after connecting does not help because without the signature check the peer is never proven to own the certificate it presents.	2026-08-14	9.1	CVE-2026-49457
bestwebsoft--Gallery by BestWebSoft Customizable Image and Photo Galleries for WordPress	The Gallery by BestWebSoft plugin for WordPress is vulnerable to SQL Injection via the `_gallery_order_{post_id}` parameter array keys in all versions up to, and including, 4.7.9. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. The `gllr_save_postdata()` function stores unsanitized array keys from `\$_POST` directly into post meta, which are later used in SQL queries without prepared statements. This makes it possible for authenticated attackers, with Editor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-16	7.2	CVE-2026-2497
bluemediapl--Autopay	The Platnosci Online Blue Media (Autopay) plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 5.0.0 via the `bm_woocommerce_css_editor_content` POST parameter. This is due to the `Css_Editor::handle_save()` method being wired to the WordPress `init` hook by `Settings_Manager::init_once()` with no capability check, no nonce verification, and no sanitization on the input - the raw `\$_POST` value is written to the `woocommerce_bluemediapl_settings` option via `update_option()`, then later echoed directly inside a <style> block on the WooCommerce checkout page by `Css_Frontend::print_to_wp_head()` with no output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page (the checkout page).	2026-08-16	7.2	CVE-2026-15002
boldgrid--W3 Total Cache	The W3 Total Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Author Name in all versions up to, and including, 2.10.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability is only exploitable when the Lazy Load Images feature of W3 Total Cache is enabled, as the unsafe re-emission occurs exclusively within the LazyLoad mutator's img tag rewriting step.	2026-08-14	7.2	CVE-2026-18109
Booking Activities Team--Booking Activities	Unauthenticated PHP Object Injection in Booking Activities <= 1.18.4 versions.	2026-08-13	8.8	CVE-2026-28176
BookingWP--WooCommerce Appointments	Unauthenticated Sensitive Data Exposure in WooCommerce Appointments <= 5.3.8 versions.	2026-08-13	7.5	CVE-2026-66462
bracketweb--Agrion	Unauthenticated Cross Site Scripting (XSS) in Agrion <= 1.0.0 versions.	2026-08-13	7.1	CVE-2026-65580

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Brainstorm Force--SureDash	Unauthenticated Cross Site Scripting (XSS) in SureDash <= 1.10.1 versions.	2026-08-13	7.1	CVE-2026-66698
browserslist--browserslist	Browserslist is a configuration tool for sharing target browsers and Node.js versions between front-end tools. Prior to 4.28.7, normalizeStats() in node.js, reached unconditionally through getStat() and loadStat() on every browserslist() call, processes untrusted browserslist-stats.json, opts.stats, and CLI --stats data with an unguarded for...in loop and plain-object bracket access and assignment, allowing inherited Object.prototype keys including __proto__, toString, valueOf, constructor, hasOwnProperty, and isPrototypeOf to cause an uncaught TypeError or modify the prototype of the returned normalized object. This issue is fixed in version 4.28.7.	2026-08-11	7.5	CVE-2026-73088
browserslist--browserslist	Browserslist is a configuration tool for sharing target browsers and Node.js versions between front-end tools. Prior to 4.28.7, index.js retains every distinct `(queries, context)` result in cache and every parseQueries() AST in parseCache without a size cap, TTL, or eviction, allowing an attacker who can influence repeated browserslist() query values, including valid since ` <year>>=<month>=<day>` queries, to bypass the caller-controlled BROWSERSLIST_DISABLE_CACHE mitigation and cause linear memory growth followed by an out-of-memory process crash. This issue is fixed in version 4.28.7.</year>	2026-08-11	7.5	CVE-2026-73089
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.40.0, the MySQL integration component in Budibase is configured with multipleStatements: true, enabling execution of multiple SQL statements in a single query. Attackers can inject malicious SQL commands through user input fields, leading to complete database compromise. This vulnerability is fixed in 3.40.0.	2026-08-12	9.6	CVE-2026-73300
Budibase--budibase	Budibase versions before 3.40.0 contain an authorization/authentication bypass in the PUT /api/global/users/tenant/owner (changeTenantOwnerEmail) endpoint. On self-hosted instances (SELF_HOSTED or DISABLE_ACCOUNT_PORTAL set), the cloudRestricted middleware is a no-op and the route is protected only by a general authentication check, so any authenticated user - including a lowest-privilege BASIC app user - can reassign the tenant account-holder (top-privilege admin) email to an attacker-controlled address. The attacker can then use the public password-reset flow to take over the admin account, leading to full administrative access.	2026-08-13	8.1	CVE-2026-72856
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.40.0, POST /api/v2/email on account.budibase.app accepted a client-controlled accountId without binding it to the authenticated session, while checking only currentEmail. An authenticated attacker who obtains a victim account identifier can start the email-change workflow for the victim, receive and submit the verification code through POST /api/v2/email/verification, move the victim email to an attacker-controlled address, and complete a password reset as the victim. This issue is fixed in version 3.40.0.	2026-08-12	8.2	CVE-2026-73303
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.24, POST /api/public/v1/roles/assign called validateGlobalRoleUpdate without checking appBuilder.appId or role.appId in packages/server/src/api/controllers/public/globalRoleValidation.ts. An app-scoped builder could scope the request to an app they control and then grant themselves builder access or an arbitrary role in another app, exposing that app data, datasource configuration, and automations. This issue is fixed in version 3.39.24.	2026-08-13	8.8	CVE-2026-73305
Budibase--budibase	Budibase before 3.40.0 contains a SQL injection vulnerability in the Oracle datasource connector's post-write row lookup that fails to escape table names in identifiers. Attackers with write permission on a table with a double-quote in its name can inject SQL that executes as the datasource's database user to read or modify arbitrary data.	2026-08-13	7.6	CVE-2026-72853
Budibase--budibase	Budibase before 3.40.0 fails to redact datasource credentials stored in STRING typed fields, allowing authenticated users to read MongoDB connection strings and Firebase private keys in plaintext. Attackers with table read permissions can retrieve datasource configurations through the read API to obtain live backend database credentials and service account keys.	2026-08-13	7.7	CVE-2026-72857
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.32, GET /api/global/users/tenant/:id was listed in PUBLIC_ENDPOINTS in packages/worker/src/api/index.ts, and tenantUserLookup returned a full PlatformUser document. An unauthenticated caller could query an email or user identifier, distinguish existing users from missing users, and obtain tenant	2026-08-12	7.5	CVE-2026-73406

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	identifiers, user identifiers, email addresses, SSO identifiers, and document revision metadata. This issue is fixed in version 3.39.32.			
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.18, packages/server/src/integrations/mysql.ts enabled multipleStatements and inserted an unescaped tableName into a DESCRIBE statement. An attacker able to create a MySQL table with a backtick and stacked statement in its name could wait for a Budibase administrator to run schema discovery, causing the second statement to execute. The fix applies quoteMySqlIdentifier before constructing the query. This issue is fixed in version 3.39.18.	2026-08-13	7.6	CVE-2026-73408
budibase--server	Budibase before 3.40.0 contains an unauthenticated SQL injection vulnerability in webhook-triggered automations with EXECUTE_QUERY steps. Attackers can POST attacker-controlled JSON to the webhook trigger endpoint to inject SQL payloads that execute with builder-configured database credentials, enabling data exfiltration, modification, and persistence in connected datasources like Snowflake.	2026-08-13	10	CVE-2026-72851
budibase--server	Budibase before 3.40.0 fails to properly sanitize S3 object keys, allowing authenticated builders to upload files with traversal sequences that are preserved during export. Attackers can craft filenames containing .. segments that escape the temporary directory during workspace export, writing arbitrary content to any path writable by the Budibase process.	2026-08-13	9.1	CVE-2026-72850
budibase--server	Budibase before 3.40.0 contains server-side request forgery vulnerabilities in OpenAPI query import and REST query execution that allow authenticated builder-level users to bypass DNS pinning protections through DNS rebinding attacks. Attackers can configure hostnames that resolve to public addresses during validation but resolve to loopback or private addresses during actual connection, allowing access to blocked internal HTTP services.	2026-08-13	8.5	CVE-2026-72855
budibase--server	Budibase Server before 3.40.0 contains a NoSQL injection vulnerability in the MongoDB query execution endpoint where user-supplied parameters are interpolated into JSON query templates without proper sanitization of JSON metacharacters. Attackers with query write permission can inject JSON structural characters to alter MongoDB queries, bypassing filters to read, modify, or delete arbitrary documents.	2026-08-13	8.3	CVE-2026-73618
budibase--server	Budibase before 3.40.0 contains a cross-site request forgery vulnerability in the chat-link handoff endpoint that allows attackers to bind an external chat identity to a victim's account. Attackers can craft a phishing page that auto-submits a POST request with a leaked confirmation token to bind their chat identity to a victim user's account, enabling impersonation within agent operations and inheritance of victim permissions.	2026-08-13	7.7	CVE-2026-72849
budibase--server	Budibase versions 3.39.4 before 3.40.0 contain an authorization regression in the S3 attachment upload endpoint that allows BASIC users to obtain S3 PutObject presigned URLs by sending POST requests to the attachments endpoint. The route was changed from a BUILDER permission check to a TABLE/WRITE check, which BASIC users hold by default. Attackers can specify arbitrary S3 buckets in the request body to generate presigned URLs for writing to any bucket accessible by the stored IAM credentials, enabling unauthorized file uploads.	2026-08-14	7.7	CVE-2026-72859
budibase--server	Budibase before 3.40.0 contains a NoSQL injection vulnerability in the MongoDB datasource integration where user-supplied parameters are enriched with handlebars using noEscaping: true and parsed without operator filtering. Attackers can inject MongoDB operators through query parameters to bypass per-user access controls, read arbitrary documents, execute JavaScript via \$where operators, or modify collections through update and delete operations.	2026-08-13	7.1	CVE-2026-73617
cachethq--cachet	Cachet through 2.4.1 contains a server-side template injection vulnerability in incident template rendering that allows authenticated users to execute arbitrary PHP code. Attackers can create malicious incident templates with Blade directives or Twig filters that execute system commands when incidents are created, achieving remote code execution as the web server process.	2026-08-10	8.8	CVE-2026-69118
Cal.com--Cal.com Self-Hosted (Cal.diy)	Cal.com Cal.diy versions 2.1.1 through 6.2.0 contain a stored cross-site scripting vulnerability in the BookingPageTagManager component that allows authenticated event owners to inject arbitrary JavaScript by supplying a malicious analytics tracking ID without sanitization. Attackers can close the inline script string literal with a crafted payload that executes in the browser of every visitor to the affected public booking page, enabling session cookie theft, forged authenticated requests, and wormable propagation by chaining with CSRF-able endpoints to persist payloads on additional events.	2026-08-12	8.9	CVE-2026-57858

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Canonical--LXD	An authorization bypass vulnerability in LXD allows an authenticated attacker to bypass target project security restrictions during cross-project instance migrations. When moving an instance cross-project to a different cluster member via POST /1.0/instances/{name} with migration: true, project: <target>, and target: <member>, the destination node skips all project restriction checks because the request arrives as an internal cluster notification. An attacker can exploit this to introduce disallowed instance configurations into a restricted project.	2026-08-12	9.9	CVE-2026-62420
Canonical--LXD	A link following vulnerability in LXD allows an attacker to achieve arbitrary file read and write operations on the host system. When importing or unpacking an image archive, LXD fails to validate whether the metadata.yaml file is a symbolic link. An attacker can exploit this flaw by providing a crafted image archive with a symlinked metadata.yaml file pointing to target file paths on the host system.	2026-08-12	9.9	CVE-2026-63293
Canonical--LXD	A link following vulnerability in LXD allows an attacker to achieve root command execution on the host system. During the import or unpacking of crafted image or backup archives, LXD fails to properly validate and confine the backup.yaml file when it exists as a symbolic link. An attacker can exploit this flaw by providing a malicious archive with a symlinked backup.yaml file, causing LXD to process unconfined configuration metadata and execute arbitrary commands with root privileges.	2026-08-12	9.9	CVE-2026-63294
Canonical--LXD	An authorization bypass vulnerability in LXD allows an authenticated attacker to bypass target project restrictions during instance migration. When migrating an instance to a target project, LXD accepts configuration overrides without validating the new configuration against the target project's enforced restrictions. An attacker can exploit this flaw to move instances with disallowed high-privilege configurations into restricted projects, bypassing security controls.	2026-08-12	9.9	CVE-2026-63296
Canonical--LXD	An authorization bypass vulnerability in LXD due to a timing flaw during configuration merging allows an authenticated attacker to bypass target project restrictions during cross-project instance copies. When copying an instance to a target project, LXD performs restriction checks before configuration merging is complete, creating a time-of-check to time-of-use (TOCTOU) condition. An attacker can exploit this flaw to copy instances with disallowed high-privilege configurations into restricted projects, bypassing security controls.	2026-08-12	9.9	CVE-2026-63297
Canonical--LXD	An improper validation vulnerability in the instancePostMigration function in lxd/instance_post.go of LXD allows an authenticated attacker with can_create_instances permissions on a restricted project to bypass project-level security restrictions. When migrating an instance between projects, LXD fails to validate the instance's configuration against the target project's enforced restrictions (such as restricted.containers.lowlevel, restricted.devices.*, and restricted.networks.access). An attacker can exploit this by creating a disallowed or high-privilege instance in an unrestricted project and subsequently moving it into the restricted project.	2026-08-12	9.9	CVE-2026-63300
Canonical--LXD	A path traversal vulnerability in LXD allows an attacker to manipulate file system paths during backup import and restore operations. When importing or restoring a backup archive, LXD fails to validate instance and storage volume names contained within the archive metadata. An attacker can exploit this flaw by supplying a crafted backup archive with malicious instance or volume names containing path traversal sequences, potentially allowing file access or overwriting outside the designated restore directory.	2026-08-12	9.9	CVE-2026-66898
Canonical--LXD	A path traversal vulnerability in LXD allows an attacker to achieve arbitrary host file read or unconstrained file creation. When processing image metadata templates, LXD fails to properly sanitize or restrict template file paths from escaping the instance templates directory (specifically affecting virtual machine / QEMU driver execution paths). An attacker can exploit this flaw by providing a crafted image archive with malicious template directives containing path traversal sequences, causing LXD to access or write files outside the intended template directory on the host system.	2026-08-12	8.5	CVE-2026-16033
Canonical--LXD	An improper neutralization of special elements vulnerability in LXD's NVIDIA instance configuration handling allows an authenticated attacker to inject arbitrary configuration directives. By supplying newline characters within the 'nvidia.driver.capabilities' or 'nvidia.require.*' configuration values, an attacker can manipulate the generated lxc.conf file. This flaw enables the attacker to execute arbitrary code on the host system with the privileges of the LXD daemon.	2026-08-12	8.7	CVE-2026-63298
Canonical--LXD	An authorization bypass vulnerability in LXD allows an authenticated user to bypass project-level disk and volume limits. Two related code paths fail to verify resource	2026-08-12	8.5	CVE-2026-63299

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	limits during volume operations: the storagePoolVolumeTypePostMove function omits the limits.AllowVolumeCreation check before moving a volume across projects, and volume snapshot restore operations skip the AllowVolumeUpdate check when the configuration is nil (Config == nil). An attacker can exploit these flaws to allocate storage resources that exceed the administrative limits configured for a project.			
cedar-policy--authorization-for-expressjs	@cedar-policy/authorization-for-expressjs is an open-source Express.js middleware that integrates Cedar authorization into Express applications by mapping HTTP requests to Cedar actions and evaluating authorization policies before allowing requests to proceed. Versions prior to 0.3.0 have an issue where, under certain circumstances, the middleware matches incoming requests against Cedar action mappings using req.originalUrl, which includes the query string, while Express routes requests using only the path component. The middleware uses req.originalUrl to match incoming requests against Cedar action mappings. In Express, req.originalUrl includes the query string, while route matching uses only the path. This creates a divergence between what Cedar authorizes and what Express executes. When an application defines separate actions for overlapping path prefixes with different authorization requirements (for example, GET /users for listing all users with admin-only access, and GET /users/{id} for retrieving a single user with any authenticated user access), an actor can append a query string to bypass the more restrictive policy. Sending GET /users/?x=1 causes the middleware to match against /users/{id} (with id parameter set to ?x=1) and evaluate the less restrictive action, while Express routes the request to the /users list handler. This allows inappropriate access to the more restrictive endpoint. This issue has been addressed in version 0.30. Some workarounds are available. Validate and sanitize incoming request paths before they reach the authorization middleware. Ensure that applications do not rely solely on the middleware for authorization when defining multiple actions on overlapping path prefixes with different permission levels.	2026-08-12	8.8	CVE-2026-49473
cedcommerce--Wholesale Market	The Wholesale Market plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 2.2.2 via the ced_wholesale_request_send AJAX action. The ced_wholesale_request_send_callback() handler only verifies a nonce (which is exposed to any authenticated user through wp_localize_script on the frontend) and that the caller has a positive user ID, then calls WP_User::add_role() with the client-supplied role_required POST parameter without restricting the value to an allowlist of wholesale roles. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to Administrator when the site administrator has enabled the 'Assigning requested role directly' option.	2026-08-15	8.8	CVE-2026-14279
Chaskiq--Chaskiq	A missing authentication vulnerability in Chaskiq through commit 46dfdd1 allows unauthenticated remote attackers to mint Stripe Billing Portal sessions for any tenant via the stripeCustomerPortal GraphQL mutation. The mutation performs no authentication or authorization checks before creating a customer portal session linked to any tenant Stripe account. An attacker can access and manage subscription data for any tenant without credentials.	2026-08-11	8.2	CVE-2026-72535
Chaskiq--Chaskiq	A missing authentication vulnerability in Chaskiq through commit 46dfdd1 allows unauthenticated remote attackers to manipulate any tenant Stripe subscription via the stripeCreateIntent GraphQL mutation. The mutation lacks authentication and authorization checks, exposing Stripe payment intent creation to unauthenticated callers. An attacker can create payment intents and alter billing for any tenant without credentials.	2026-08-11	8.2	CVE-2026-72536
Chocoboazz--PeerTube	PeerTube is an ActivityPub-federated video streaming platform. Prior to 8.2.2, processUpdateActivity and processUpdateVideo accept an ActivityPub Update containing a Video object without verifying that byActor.url is authorized for the host in videoObject.id, allowing a malicious federated server to rewrite another server's video metadata, visibility, media file, and HLS URLs. This issue is fixed in version 8.2.2.	2026-08-11	9.3	CVE-2026-73090
Chocoboazz--PeerTube	PeerTube is an ActivityPub-federated video streaming platform. Prior to 8.1.6, ActorFollowModel.updateScore() interpolates the attacker-controlled ActivityPub actor inboxUrl into an SQL query, allowing an unauthenticated remote server to read and write PeerTube database tables, including oAuthToken.accessToken, and take over administrator accounts. This issue is fixed in version 8.1.6.	2026-08-11	9.8	CVE-2026-73211
cisagov--Malcolm	Malcolm is a network traffic analysis tool suite. The file-upload component (FilePond PHP backend) accepts uploads at `POST /server/php/submit.php` and	2026-08-11	8.8	CVE-2026-55676

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stores them in a directory served by the same nginx and php-fpm instance. The allow-list that should restrict accepted file types is an empty array by default (`file-upload/php/config.php:16`), so the type check is a no-op and every extension is accepted. The filename sanitizer keeps the `.php` extension intact. Committed files land in `/var/www/upload/server/php/files` (`file-upload/php/config.php:7`), and the component's nginx routes any URL ending in `.php` to php-fpm. An authenticated `GET /server/php/files/<name>.php` then executes the uploaded code as `www-data`. Prior to version 26.06.1, in RBAC mode, the upload endpoint is reachable by the granular `ROLE_UPLOAD` role (`nginx/lua/nginx_auth_helpers.lua:71`), a role intended only for submitting capture files. As a result, a user holding the upload-only role runs arbitrary PHP as `www-data` inside the file-upload container. Version 26.06.1 fixes the issue.			
cisagov--Malcolm	Malcolm is a network traffic analysis tool suite. Prior to version 26.07.0, role-based access control enforced in the Nginx OpenResty Lua layer evaluates the raw, unnormalized `ngx.var.request_uri`, while Nginx itself routes requests using the normalized path. An authenticated low-privilege user can prepend a traversal segment (for example `/x/./upload/...`) so that Nginx routes the request to a restricted backend while the Lua role check fails to match any rule and falls open, granting access it should deny. Version 26.07.0 fixes the issue.	2026-08-11	7.1	CVE-2026-63177
Cisco--Cisco Secure Firewall Adaptive Security Appliance (ASA) Software	A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient error checking when processing HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to the Remote Access SSL VPN service on an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2026-08-11	8.6	CVE-2026-20349
CiviCRM--CiviCRM	An SQL injection vulnerability in CiviCRM through 6.18.alpha1 allows authenticated staff to read the entire database via the contact search RLIKE clause. The clause concatenates a user-supplied value into the SQL query without sanitization. An attacker with staff-level access can exfiltrate all database contents including donor and member records.	2026-08-11	8.8	CVE-2026-72558
Cloudflare-- https://github.com/cloudflare/pages-action	Description Cloudflare was recently notified by external researchers of vulnerabilities in this archived repository, including a remote code execution issue in `src/index.ts` reachable from certain GitHub Actions workflow configurations. Successful exploitation may expose workflow secrets such as CLOUDFLARE_API_TOKEN and GITHUB_TOKEN to an attacker. Because this repository has been deprecated since 2024, Cloudflare will not be issuing patches. To remediate this issue, we recommend migrating to `cloudflare/wrangler-action` immediately. Consumers who have already migrated are not affected. Sunset Date The cloudflare/pages-action repository will be removed on 2026-09-18. Consumers must complete migration before 18th September to avoid CI disruption. Affected Versions All published versions of cloudflare/pages-action, including consumers pinned to the v1 moving tag. Patched Versions None. This repository will not receive further updates, including security patches. Resolution / Migration Path Migrate all workflows using cloudflare/pages-action to `cloudflare/wrangler-action` before 2026-09-18. Refer to the wrangler-action README for the equivalent step configuration and migration guidance. Credit Thanks to @agentka99 and @beg1nn3r for reporting their findings via Cloudflare's HackerOne program that informe	2026-08-12	8.8	CVE-2026-11325
Cockpit CMS--Cockpit CMS	An unrestricted file upload vulnerability in Cockpit CMS 2.6.0 allows authenticated users to upload files of any extension including PHP scripts via the asset upload endpoint. The allowed_uploads configuration defaults to wildcard (*) and uploaded files are stored in a web-accessible directory. An attacker with any authenticated account can upload a PHP webshell and execute arbitrary OS commands on the server.	2026-08-11	8.8	CVE-2026-72557
Cockpit HQ--Cockpit CMS	Cockpit CMS 2.14.0 and prior contains a command injection vulnerability in the FFmpeg integration that allows authenticated users with only the assets/upload permission to execute arbitrary commands by uploading a video file with a shell metacharacter-laden filename. The unsanitized filename is interpolated into a shell command executed via Process::fromShellCommandline() before the slugify() sanitizer runs, enabling injected shell metacharacters such as backticks, \$(), and	2026-08-14	8.8	CVE-2026-73680

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	semicolons to escape the FFmpeg command context and execute as the web-server user.			
code-projects--Online Shopping System	A vulnerability was found in code-projects Online Shopping System 1.0. This impacts an unknown function of the file /login.php of the component Login. The manipulation of the argument email results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	2026-08-15	7.3	CVE-2026-19919
CODEPRESS--Visitor Traffic Real Time Statistics Pro	Subscriber SQL Injection in Visitor Traffic Real Time Statistics Pro <= 11.10 versions.	2026-08-13	8.5	CVE-2026-66430
CODEPRESS--Visitor Traffic Real Time Statistics Pro	Unauthenticated Cross Site Scripting (XSS) in Visitor Traffic Real Time Statistics Pro <= 11.10 versions.	2026-08-13	7.1	CVE-2026-66429
Colissimo--Colissimo Officiel : Mthodes de livraison pour WooCommerce	Unauthenticated Cross Site Scripting (XSS) in Colissimo Officiel : MÃ©thodes de livraison pour WooCommerce <= 2.10.0 versions.	2026-08-13	7.1	CVE-2026-66697
connectordev--bLoyal: Loyalty & Promotions by bLoyal	The bLoyal: Loyalty & Promotions by bLoyal plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.1.611.78. This is due to the AJAX actions `save_bloyal_configuration_data` and `save_bloyal_accesskeyverification_data` being registered without any capability or nonce checks, and the `bloyal_customer_auto_login` function unconditionally trusting the `Customer.ExternalId` value returned by whichever API URL is stored in the plugin's options. This makes it possible for authenticated attackers, with Subscriber-level access and above, to overwrite the plugin's bLoyal Loyalty Engine API URL (`bloyal_custom_loyaltyengine_api_url`) and the `is_bloyal_custom_api_url` flag via the unprotected AJAX actions, then trigger the unauthenticated `/cart` REST route to cause `bloyal_customer_auto_login` to fetch customer data from an attacker-controlled endpoint and call `wp_set_auth_cookie()` with an attacker-supplied `Customer.ExternalId`, thereby authenticating as any WordPress user including the site Administrator.	2026-08-15	8.8	CVE-2026-15001
cozmoslabs--User Profile Builder Beautiful User Registration Forms, User Profiles & User Role Editor	The User Profile Builder plugin for WordPress is vulnerable to Authentication Bypass via Type Confusion in versions up to, and including, 3.16.4. This is due to the wppb_log_in_user() function calling absint() on the return value of wp_insert_user() before performing an is_wp_error() check - when a registration is submitted with a 61-70 character username, WordPress core rejects it with a WP_Error object, but absint() coerces that object to the integer 1 before the error check can short-circuit execution, causing the plugin to bind and return a transient-backed autologin nonce tied to user ID 1. This makes it possible for unauthenticated attackers to log in as the site's Administrator account (user ID 1), resulting in full administrative takeover of the site.	2026-08-15	9.8	CVE-2026-15826
Cozy Vision Technologies Pvt. Ltd.--SMS Alert Order Notifications	Unauthenticated Privilege Escalation in SMS Alert Order Notifications <= 3.9.7 versions.	2026-08-13	9.8	CVE-2026-66424
craftcms--cms	Craft CMS versions from 4.0.0-RC1 before 4.18.2 and from 5.0.0-RC1 before 5.10.6 contain an authenticated remote code execution vulnerability in the control panel element-search condition handling. Craft cleanses the outer request-controlled condition array via Component::cleanseConfig(), but Conditions::createCondition() later decodes and merges the JSON string in condition.config without re-running cleanseConfig() on the decoded configuration. Because condition.config is a JSON string during the first cleanse, Yii special config keys such as 'as ...' and 'on ...' can be hidden inside it and, after JSON decoding, are interpreted by Yii as behavior/event configuration during FieldLayout object creation. An attacker with an authenticated control panel session (and a valid CSRF token) can exploit this to execute operating system commands as the PHP/web user.	2026-08-11	8.8	CVE-2026-72778
craftcms--cms	Craft CMS versions >= 5.0.0-RC1 before 5.10.7 and >= 4.0.0-RC1 before 4.18.3 contain a remote code execution vulnerability in the Twig sandbox mechanism. Because Craft marks the ElementInterface as safe (via the AllowedInSandbox attribute) and the sandbox allowlisting extends to the entire class hierarchy (craft\base\Component up to yii\base\Component), an authenticated attacker with permission to access the control panel can render a malicious Twig template that abuses the yii\base\Component arbitrary function-call gadget to execute arbitrary code, even when the Twig sandbox is enabled via enableTwigSandbox().	2026-08-11	8.8	CVE-2026-72781

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
CSZ CMS--CSZ CMS	A broken access control vulnerability in CSZ CMS 1.3.2 allows unauthenticated remote attackers to read all form submissions including personally identifiable information via the admin form-submission viewer. The viewer endpoint lacks an authentication check and the framework authentication helper fails open. An unauthenticated attacker can access all contact form submissions without credentials.	2026-08-11	7.5	CVE-2026-72601
cube-root--directory-serve	A path traversal vulnerability in cube-root/directory-serve through 1.3.7 allows an unauthenticated remote attacker to delete arbitrary files outside the intended served directory when the application is run with the --delete option.	2026-08-10	9.1	CVE-2026-72569
Daan.dev--OMGF Pro	Unauthenticated Arbitrary File Download in OMGF Pro <= 5.2.7 versions.	2026-08-13	7.5	CVE-2026-61980
daggerhart--Query Wrangler	The Query Wrangler plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.5.57 via the 'options' parameter parameter. This is due to missing capability check and nonce verification on the wp_ajax_qw_form_ajax handler, combined with unsanitized attacker-controlled options fully replacing saved query options and being passed directly to call_user_func_array() guarded only by function_exists(). This makes it possible for authenticated attackers, with subscriber-level access and above, to execute code on the server. Exploitation requires only that at least one query row exists in the database, as the query_id is a small enumerable integer with no further access control.	2026-08-16	8.8	CVE-2026-14498
daptin--daptin	An improper authorization vulnerability in daptin through v0.12.34 allows unauthenticated remote attackers to read, create, update, and delete usergroup records. The permission check functions (CanRead, CanPeek, CanCreate, CanUpdate, CanDelete, CanRefer) in server/permission/permission.go return true whenever p.UserId equals the requesting userId, but fail to reject the null/zero reference - unlike CanExecute, which explicitly guards it.	2026-08-10	9.1	CVE-2026-72575
Dassault Systmes--SIMULIA Execution Engine	A Deserialization of Untrusted Data vulnerability affecting SIMULIA Execution Engine from Release 2023 through Release 2026 could lead to an unauthenticated remote code execution.	2026-08-11	10	CVE-2026-17061
datavane--tis	Datavane TIS v5.0.0 contains an XML external entity (XXE) injection vulnerability that allows authenticated attackers to perform server-side request forgery and out-of-band file exfiltration by supplying a crafted taskScript payload to the doEditWorkflow endpoint, which processes XML through an unhardened DocumentBuilderFactory with external entities and DTD loading enabled. Attackers can send a malicious XML document containing an external DTD reference to the edit_workflow action, causing the server to issue outbound HTTP requests to attacker-controlled infrastructure and exfiltrate local files readable by the TIS process user, including configuration files and Derby database credentials.	2026-08-14	7.7	CVE-2026-69101
DaveGamble--cJSON	cJSON versions 1.5.0 through 1.7.19 contain an incorrectly-resolved name or reference vulnerability in the decode_pointer_inplace() function within cJSON_Utils.c that allows unauthenticated attackers to cause JSON Patch operations to target wrong object keys by supplying crafted JSON Pointer escape sequences (~0 or ~1) in patch paths. Attackers can submit malicious RFC 6902 JSON Patch input to applications using cJSONUtils_ApplyPatches() or cJSONUtils_ApplyPatchesCaseSensitive() to silently corrupt data or delete unintended keys, potentially bypassing authorization controls in applications that rely on JSON Patch for access-controlled data modification.	2026-08-11	7.5	CVE-2026-29036
davila7--claude-code-templates	Claude Code Templates is a CLI tool for configuring and monitoring Claude Code. Prior to 1.29.4, the Claude Code Studio server launched by the --studio option in cli-tool/src/sandbox-server.js binds to all interfaces on port 3444, permits cross-origin requests, and requires no authentication. The POST /api/execute endpoint passes the prompt request-body field to executeLocalTask(), and POST /api/install-agent passes the agentName request-body field to a child process. The same unsafe agent field path is reachable from /api/execute through checkAndInstallAgent(). These attacker-controlled values reach child_process.spawn() with shell execution enabled, causing Node.js to construct a shell command in which metacharacters are interpreted. An attacker who can reach the port directly, or who convinces a developer running Studio to visit a malicious website, can execute arbitrary operating-system commands with the developer's privileges and compromise source code, credentials, and local data. This issue is fixed in version 1.29.4.	2026-08-11	8.8	CVE-2026-73222
DayuanJiang--next-ai-draw-io	Next AI Draw.io through 0.4.16 contains a server-side request forgery vulnerability in the POST /api/parse-url endpoint due to hostname validation that only checks	2026-08-13	8.6	CVE-2026-72777

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	string patterns without DNS resolution. Unauthenticated attackers can supply hostnames that bypass string validation but resolve to internal addresses, allowing them to reach arbitrary internal HTTP services and exfiltrate responses including cloud metadata.			
Dell--Display and Peripheral Manager (DDPM Windows)	Dell Display and Peripheral Manager (DDPM Windows), versions prior to 2.3.0.17, contain an Authentication Bypass by Spoofing vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges and arbitrary code execution.	2026-08-12	7.8	CVE-2026-46731
Dell--Display and Peripheral Manager (DDPM Windows)	Dell Display and Peripheral Manager (DDPM Windows), versions prior to 2.3.0.17, contain an Authentication Bypass by Spoofing vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges and arbitrary code execution.	2026-08-12	7.8	CVE-2026-59914
Dell--Display and Peripheral Manager (DDPM Windows)	Dell Display and Peripheral Manager (DDPM Windows), versions prior to 2.3.0.17, contain Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges and arbitrary code execution.	2026-08-12	7.8	CVE-2026-59916
Dell--Display and Peripheral Manager (DDPM Windows)	Dell Display and Peripheral Manager (DDPM Windows), versions prior to 2.3.0.17, contain Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges and arbitrary code execution.	2026-08-12	7.8	CVE-2026-59917
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to 2605.0.2, contain an Incorrect Default Permission vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Privilege Escalation.	2026-08-14	7.8	CVE-2026-63700
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to 2605.0.2, contain an Unrestricted Upload of File with Dangerous Type vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote Code Execution.	2026-08-14	7.2	CVE-2026-66270
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to 2605.0.2, contain an Unrestricted Upload of File with Dangerous Type vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote Code Execution.	2026-08-14	7.2	CVE-2026-66271
denishua--WPJAM Basic	Subscriber SQL Injection in WPJAM Basic <= 7.0.1 versions.	2026-08-13	9.3	CVE-2026-61966
denishua--WPJAM Basic	Subscriber Sensitive Data Exposure in WPJAM Basic <= 7.0.2.1 versions.	2026-08-13	7.5	CVE-2026-66432
Dimitri Grassi--Salon booking system	Unauthenticated Broken Authentication in Salon booking system <= 10.30.26 versions.	2026-08-13	9.8	CVE-2026-66453
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, the Rich Text Editor rendered a chat-transcript username as HTML, allowing stored cross-site scripting. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-10	8.7	CVE-2026-72730
discourse--discourse	Discourse is an open-source discussion platform. From 2026.1.0-latest until 2026.1.7, 2026.6.2, 2026.7.1, and 2026.8.0-latest.1, anyone able to run a parameterized Data Explorer query, including non-staff members of a group a query is shared with, could craft parameter values that escaped the intended query and executed arbitrary SQL through plugins/discourse-data-explorer/lib/discourse_data_explorer/data_explorer.rb and plugins/discourse-data-explorer/lib/discourse_data_explorer/workflows/sql_action/v1.rb. Recursive parameter interpolation allowed one parameter value to introduce another parameter, and parameter declarations in SQL comments could be used to inject a statement. Queries run in a read-only transaction, so data could not be modified, but any table could be read. This issue is fixed in versions 2026.1.7, 2026.6.2, 2026.7.1, and 2026.8.0-latest.1.	2026-08-10	7.1	CVE-2026-72731
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the backup.restoreBackupWithLogs tRPC subscription builds database restore shell pipelines from the user-controlled databaseName and backupFile fields without safely separating them from shell syntax. packages/server/src/utls/restore/utls.ts interpolates databaseName into database-specific restore commands, while packages/server/src/utls/restore/postgres.ts and the analogous restore modules interpolate backupFile into rclone paths. An authenticated member with backup-restore permission can inject operating-system commands that execute in the Dokploy host context through execAsync or execAsyncRemote, even when no valid database container or backup file exists. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72733

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, writeTraefikConfigRemote in packages/server/src/utils/traefik/application.ts serializes user-controlled Traefik configuration with yaml.stringify and interpolates the resulting yamlStr into an echo command executed through execAsyncRemote. Single quotes in redirect regex and replacement fields, basic authentication usernames, domain host values, or middleware configuration can terminate the shell quoting and execute arbitrary commands on managed remote servers with the configured SSH user's privileges. This vulnerability is caused by an incomplete fix for CVE-2026-45630. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72735
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, Dokploy passes user-controlled values directly into shell commands via unquoted template literal interpolation in the registry credential testing and Docker Swarm cluster management endpoints. Both endpoints have a safe local code path (using execFileAsync or the Docker API) but a vulnerable remote path (using execAsyncRemote which runs the shell string via SSH). This vulnerability is fixed in 0.29.13.	2026-08-10	9.9	CVE-2026-72736
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.29.8 and earlier, backup.create, backup.update, and backup.restoreBackupWithLogs in apps/dokploy/server/api/routers/backup.ts accept a client-controlled destinationId and use the referenced destination without verifying that destination.organizationId equals ctx.session.activeOrganizationId. An authenticated member with backup permissions for a service in one organization can cause another organization's S3 accessKey and secretAccessKey to be materialized by packages/server/src/utils/backups/utils.ts getS3Credentials on the attacker's service host, read that organization's backup objects, or redirect and poison backups across tenant boundaries.	2026-08-10	9.6	CVE-2026-72737
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the backup.listBackupFiles tRPC endpoint in apps/dokploy/server/api/routers/backup.ts passes the search parameter through normalizeS3Path and interpolates it into an rclone lsjson command executed by child_process.exec(), allowing an authenticated user with backup:read permission to execute arbitrary commands on the Dokploy host. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72738
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, packages/server/src/utils/providers/git.ts parses the user-controlled customGitUrl with sanitizeRepoPathSSH and interpolates its domain into the ssh-keyscan command from addHostToKnownHostsCommand without shell quoting, allowing an authenticated member with service deployment permission and an attached SSH key to execute arbitrary commands on the Dokploy host during deployment. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72740
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the mariadb.ts, mongo.ts, mysql.ts, postgres.ts, redis.ts, and libsql.ts Dokploy database service deployment functions pass user-controlled dockerImage fields unquoted into docker pull \${dockerImage} shell commands on the remote-server code path. This vulnerability is fixed in 0.29.13.	2026-08-10	9.9	CVE-2026-72862
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, Dokploy's WebSocket handlers (in-app terminals and log streamers) authenticate the session but never authorize it. They establish who the user is via validateRequest() and then proceed without consulting the role/permission model that every tRPC procedure enforces. Any authenticated member, can therefore open an interactive shell into any container on the host, including the dokploy container that mounts the Docker socket, and from there obtain root on the host, escaping the application and crossing every tenant boundary. This vulnerability is fixed in 0.29.13.	2026-08-10	9.9	CVE-2026-72863
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the local branch of /docker-container-terminal in apps/dokploy/server/wss/docker-container-terminal.ts authenticates with validateRequest but does not authorize the attacker-controlled containerId against the caller's role, organization, or service access before passing it to `docker exec`, allowing any authenticated member to obtain a root shell in arbitrary containers on a self-hosted instance. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72864
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the compose.update operation stores an unvalidated composePath that packages/server/src/utils/builders/compose.ts and	2026-08-10	9.9	CVE-2026-72865

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	packages/server/src/services/compose.ts interpolate into docker compose -f, docker stack deploy -c, and touch shell commands executed through /bin/sh -c. An authenticated member with compose write and deploy permission can supply a crafted composePath, trigger compose.deploy or startCompose, and execute arbitrary operating-system commands in the Docker-privileged Dokploy host context. This issue is fixed in version 0.29.13.			
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). From 0.29.3 until 0.29.13, the incomplete fix for CVE-2026-45628 leaves packages/server/src/db/schema/compose.ts branch fields without server-side validation, allowing a direct compose.update request to store a malicious customGitBranch, branch, gitlabBranch, bitbucketBranch, or giteaBranch. A low-privileged authenticated user can trigger compose.deploy, which passes the stored branch to shell-based Git clone commands in packages/server/src/utls/providers/git.ts, github.ts, gitlab.ts, bitbucket.ts, and gitea.ts, resulting in arbitrary host command execution. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72867
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, apps/dokploy/server/api/routers/destination.ts interpolates the accessKey, secretAccessKey, region, endpoint, provider, and bucket fields from destination.testConnection into an rclone ls command executed through child_process.exec. The `withPermission("destination", "create")` path permits a low-privileged organization member to reach the mutation, close a quoted argument with a crafted field, and execute arbitrary commands in the root Dokploy container, which has access to the host Docker socket. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72868
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the backup.restoreBackupWithLogs tRPC subscription passes the databaseName parameter to restore builders in packages/server/src/utls/restore/utls.ts, where PostgreSQL, MariaDB, MySQL, and MongoDB commands embed the value in nested shell text executed by Node.js exec. An authenticated user with backup:restore permission can supply a crafted databaseName that the host /bin/sh expands before docker exec, resulting in arbitrary commands running in the Docker-privileged host context. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72869
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, application.saveBitbucketProvider stores bitbucketOwner and bitbucketRepository without validation and cloneBitbucketRepository in packages/server/src/utls/providers/bitbucket.ts interpolates those values into git clone commands executed through execAsync or execAsyncRemote, allowing a member with service deployment permission to execute arbitrary operating system commands on the Dokploy host or target server. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72872
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, swarm.getNodes, swarm.getNodeInfo, swarm.getNodeApps, and swarm.getAppInfos in apps/dokploy/server/api/routers/swarm.ts accept another organization's serverId without an activeOrganizationId ownership check, and getNodeInfo in packages/server/src/services/docker.ts interpolates nodeId into execAsyncRemote, allowing a caller with server:read permission to execute arbitrary commands as the configured SSH user on another tenant's server. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72876
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the dockerImage field is interpolated without quoting into shell commands in buildRemoteDocker() in packages/server/src/utls/providers/docker.ts and is validated only as an optional string. An authenticated user with application create or update permission can use shell command substitution in dockerImage to execute arbitrary commands on the local build host or a remote SSH build target, exposing host secrets and other projects. This issue is fixed in version 0.29.13.	2026-08-10	9.6	CVE-2026-72877
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, Dokploy's backup and restore pipeline constructs shell commands by directly interpolating user-controlled database fields into bash -c "..." and sh -c "..." strings, then executes them via child_process.exec(). An authenticated admin/owner can inject arbitrary OS commands that execute on the host machine running Dokploy (not just inside a container). This vulnerability is fixed in 0.29.13.	2026-08-10	9.6	CVE-2026-72878
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the apiCreateCertificate schema in packages/server/src/db/schema/certificate.ts	2026-08-10	9.9	CVE-2026-72880

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accepts a client-supplied certificatePath, and packages/server/src/services/certificate.ts joins that value to the certificate root without confinement. An authenticated user with certificate create or delete permission can use certificatePath to write attacker-controlled certificate content outside the intended directory or delete an out-of-root directory. This vulnerability is fixed in 0.29.13.			
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). In 0.28.8 and earlier, an authenticated user who can create or update file mounts for a service can inject shell metacharacters into filePath, causing Dokploy to execute attacker-controlled commands on the configured remote managed server over SSH. In the default deployment model, this yields direct remote host RCE from the web interface.	2026-08-10	9.9	CVE-2026-72882
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). From 0.29.2 until 0.29.13, schedule.create and schedule.update in apps/dokploy/server/api/routers/schedule.ts derive servceld from applicationId or composeld and execute the owner/admin host-schedule gate only in the alternative branch, allowing a member with access to one application to attach its applicationId to a dokploy-server schedule and run a supplied script as root through schedule.runManually. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72886
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, Dokploy allows an authenticated low-privilege member to execute arbitrary commands on the control-plane host because the volumeName field accepted by volumeBackup.create and volumeBackup.runManually is interpolated without quoting in packages/server/src/utls/volume-backups/backup.ts and executed through child_process.exec, with Docker socket access making execution host/root-equivalent. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72901
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, Dokploy allows an authenticated user to execute arbitrary commands on a local or SSH-connected target server because registry.testRegistry and registry.testRegistryById in apps/dokploy/server/api/routers/registry.ts interpolate the password field into an execAsyncRemote shell command instead of using safeDockerLoginCommand. This issue is fixed in version 0.29.13.	2026-08-10	9.9	CVE-2026-72902
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). From 0.28.7 until 0.29.13, the server.remove tRPC mutation in apps/dokploy/server/api/routers/server.ts accepts a caller-controlled serverId and calls haveActiveServices, findServerById, removeDeploymentsByServerId, and deleteServer without verifying that currentServer.organizationId equals ctx.session.activeOrganizationId. An authenticated owner or administrator with server:delete in one organization who previously observed another organization's serverId can delete that organization's server registration and deployment records, interrupt Dokploy management, and receive the associated plaintext SSH private key even though server.one denies the same cross-organization read. This issue is fixed in version 0.29.13.	2026-08-10	8.4	CVE-2026-72734
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the WebSocket handler in apps/dokploy/server/wss/terminal.ts validates a session but does not authorize access to the requested server. An authenticated user can connect to /terminal?serverId=local, select the special serverId=local branch, and obtain an interactive terminal on the Dokploy host without an organization role or server-access check. This issue is fixed in version 0.29.13.	2026-08-10	8.8	CVE-2026-72866
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, settings.readTraefikFile in apps/dokploy/server/api/routers/settings.ts passes a path accepted by apiReadTraefikConfig to readConfigInPath in packages/server/src/utls/traefik/application.ts, where configPath is interpolated into execAsyncRemote as cat \${configPath}, allowing a user with traefikFiles.read permission to execute arbitrary commands on a managed server through shell metacharacters. This issue is fixed in version 0.29.13.	2026-08-10	8.8	CVE-2026-72875
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the WebSocket handlers in apps/dokploy/server/wss/terminal.ts, apps/dokploy/server/wss/docker-container-terminal.ts, apps/dokploy/server/wss/docker-container-logs.ts, and apps/dokploy/server/wss/docker-stats.ts validate organization membership but do not enforce checkServiceAccess, accessedServerIds, or accessedServices, allowing an authenticated organization member to obtain root terminal access and read logs or statistics for restricted servers and services. This issue is fixed in version 0.29.13.	2026-08-10	8.8	CVE-2026-72883

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the unauthenticated /api/providers/github/setup route in apps/dokploy/pages/api/providers/github/setup.ts trusts gh_init organizationId and userId values from the state parameter and calls createGithub in packages/server/src/services/github.ts, allowing an attacker to insert a GitHub App provider containing client_secret, webhook_secret, and PEM private key material into another organization. This issue is fixed in version 0.29.13.	2026-08-10	7.5	CVE-2026-72871
doobidoo--mcp-memory-service	mcp-memory-service is a semantic memory layer for AI applications. Prior to 10.67.1, all HTTP routes under /api/documents/* in mcp-memory-service are served without any authentication dependency, even when the server is configured with an API key (MCP_API_KEY) or OAuth. An unauthenticated remote attacker can upload arbitrary content into the memory store (write), retrieve stored document content (read), and permanently delete memories belonging to authenticated users (delete) - all without supplying any credentials. The /api/memories counterpart correctly enforces authentication, making this an inconsistent and exploitable authentication boundary. This vulnerability is fixed in 10.67.1.	2026-08-14	9.8	CVE-2026-50027
Dromara--lamp-cloud	A vulnerability was found in Dromara lamp-cloud up to 5.10.0. This vulnerability affects unknown code of the file FileAnyoneController.java of the component File-Upload Controller. Performing a manipulation of the argument bucket/bizType results in path traversal. The attack can be initiated remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-13	7.3	CVE-2026-19757
dromara--lamp-cloud	A vulnerability was determined in dromara lamp-cloud up to 5.10.0. This issue affects some unknown processing of the file FileChunkController.java of the component chunk-check endpoint. Executing a manipulation of the argument Name can lead to path traversal. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-13	7.3	CVE-2026-19758
dromara--MaxKey	MaxKey contains an unauthorized access vulnerability due to a hard-coded JWT signing secret in application-maxkey.properties that allows unauthenticated attackers to forge valid JWT tokens and authenticate as any user by exploiting the password-skipped login endpoint. Attackers can craft a JWT token signed with the publicly known default secret, submit it to the /sign/login/jwt/trust endpoint, and obtain a fully authenticated admin session with access to SSO application configuration and downstream application secrets.	2026-08-11	9.8	CVE-2026-69102
DTStack--Taier	A vulnerability was found in DTStack Taier 1.4.0. Affected by this vulnerability is the function Paths.ge of the file FileChunkController.java of the component Chunk-Check Endpoint. The manipulation of the argument Name results in path traversal. The attack may be launched remotely. The exploit has been made public and could be used.	2026-08-14	7.3	CVE-2026-19762
Dub--Dub	A server-side request forgery vulnerability in Dub as of 2026-07-10 allows unauthenticated remote attackers to make the server issue HTTP requests to arbitrary internal or external hosts via the metatags edge endpoint. The endpoint fetches any caller-supplied URL without applying a denylist or requiring authentication. An attacker can use this to scan internal services or exfiltrate data from cloud metadata endpoints.	2026-08-11	7.5	CVE-2026-72552
duhow--xiaoai-patch	An OS command injection vulnerability in duhow/xiaoai-patch through commit fb07049 allows a remote attacker to execute arbitrary system commands on Xiaomi smart speakers running the patch. The /mute and /unmute endpoint handlers in api/main.py pass the user-supplied silent query parameter directly to os.system() without sanitization, enabling command injection via shell metacharacters.	2026-08-10	9.8	CVE-2026-72580
duhow--xiaoai-patch	A server-side request forgery (SSRF) vulnerability in duhow/xiaoai-patch through commit fb07049 allows a remote attacker to make the Xiaomi smart speaker perform HTTP requests to arbitrary internal or external URLs. The /auth endpoint in api/main.py uses the user-supplied url POST parameter to redirect to a Home Assistant instance without validating the destination URL, enabling internal network scanning and access to internal services.	2026-08-10	8.6	CVE-2026-72581
dulldusk--phpfm	An unrestricted file upload vulnerability in dulldusk/phpfm through 1.8.0 allows an unauthenticated remote attacker to execute arbitrary PHP code on the server. The application ships with an empty upload extension filter (= array) and no authentication enabled by default (auth_pass is empty string), allowing an	2026-08-10	9.8	CVE-2026-72592

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated attacker to upload a PHP webshell and execute it by browsing to the uploaded path.			
dulldusk--phpfm	A missing authentication vulnerability in dulldusk/phpfm through 1.8.0 allows an unauthenticated remote attacker to access the full file manager functionality including reading, writing, deleting, and uploading files anywhere on the server filesystem.	2026-08-10	9.8	CVE-2026-72593
Dylan Kuhn--Geo Mashup	Unauthenticated Local File Inclusion in Geo Mashup <= 1.13.18 versions.	2026-08-13	8.1	CVE-2026-66450
Dylan Kuhn--Geo Mashup	Unauthenticated Cross Site Scripting (XSS) in Geo Mashup <= 1.13.18 versions.	2026-08-13	7.1	CVE-2026-66449
e107--e107	An SQL injection vulnerability in e107 2.4.0 allows unauthenticated remote attackers to execute arbitrary SQL via the news item page ID parameter. The parameter is concatenated without escaping into a SQL WHERE clause. An unauthenticated attacker can read, modify, or delete all database contents including administrator credentials.	2026-08-11	9.8	CVE-2026-72599
echoplugins--Knowledge Base for Documentation, FAQs with AI Assistance	Unauthenticated Cross Site Scripting (XSS) in Knowledge Base for Documentation, FAQs with AI Assistance <= 17.211.0 versions.	2026-08-13	7.1	CVE-2026-28187
ECOVACS ROBOTICS--DEEBOT PRO M1	DEEBOT PRO M1 and DEEBOT PRO K1VAC leave the telnet servers enabled. The telnet service may be leveraged to log in to the affected products.	2026-08-10	8.8	CVE-2026-66405
ECOVACS ROBOTICS--DEEBOT PRO M1	DEEBOT PRO M1 and DEEBOT PRO K1VAC improperly implement authentication in WebSocket communication. The WebSocket private key may be retrieved through analyzing the traffic data via a man-in-the-middle attack, and communication contents may be altered.	2026-08-10	8.1	CVE-2026-66407
ECOVACS ROBOTICS--DEEBOT PRO M1	DEEBOT PRO M1 and DEEBOT PRO K1VAC leave the web server for debugging purposes enabled. The floor map and log information stored on the affected products may be retrieved.	2026-08-10	7.5	CVE-2026-66403
Edge-Themes--Barista	Unauthenticated Local File Inclusion in Barista <= 2.5.1 versions.	2026-08-13	8.1	CVE-2026-66653
Edimax--EW-7478APC	A weakness has been identified in Edimax EW-7478APC 1.04. This affects the function formWanTcpipSetup of the file /goform/formWanTcpipSetup. This manipulation of the argument pppUserName causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-16	9.9	CVE-2026-19959
Edimax--EW-7478APC	A vulnerability was detected in Edimax EW-7478APC 1.04. Affected is the function formWISiteSurvey of the file /goform/formWISiteSurvey. Performing a manipulation of the argument selSSID results in buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-16	9.9	CVE-2026-19961
Edimax--EW-7478APC	A security vulnerability has been detected in Edimax EW-7478APC 1.04. This impacts the function formWlbasic of the file /goform/formWlbasic. Such manipulation of the argument rootAPmac leads to command injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-16	7.4	CVE-2026-19960
Edimax--EW-7478APC	A flaw has been found in Edimax EW-7478APC 1.04. Affected by this vulnerability is the function setWAN of the file /goform/setWAN. Executing a manipulation of the argument pppUserName/ppptUserName/L2TPUserName can lead to command injection. The attack may be performed from remote. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-16	7.4	CVE-2026-19962
Edimax--EW-7478APC	A vulnerability has been found in Edimax EW-7478APC 1.04. Affected by this issue is the function stainfo of the file /goform/stainfo. The manipulation of the argument interface leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-16	7.4	CVE-2026-19963
EFM--ipTIME AX8004M	A vulnerability was determined in EFM ipTIME AX8004M 15.09.0. Impacted is the function popen of the file /cgi/d.cgi of the component CGI Endpoint. This manipulation of the argument fname causes os command injection. The attack can	2026-08-10	7.3	CVE-2026-19379

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.			
Elastic--Elasticsearch	The native inference process that Elasticsearch uses to evaluate uploaded machine learning models accepts a model operation that computes a memory address from an offset supplied inside the model, without validating that the offset stays within the bounds of the underlying storage. A user with the privileges required to upload and deploy a trained model can craft a model that reads and writes memory outside the intended allocation. The result is heap corruption that crashes the inference process, and, with sufficient control over the heap layout, could allow arbitrary code execution in the context of that process.	2026-08-13	8.8	CVE-2026-72642
Elastic--Kibana	Missing Authorization (CWE-862) in Kibana can lead to unauthorized execution of Osquery and Elastic Defend response actions on managed hosts via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). A Kibana user who is able to author and evaluate Elastic Security detection rules can cause response actions to be carried out against enrolled agents without holding the Osquery live query privileges or the Elastic Defend response action privileges that normally govern those capabilities. Depending on the response action involved, this can result in disclosure of information from the affected hosts or in unauthorized changes to their state.	2026-08-13	8.1	CVE-2026-72665
Elastic--Kibana	Authorization Bypass Through User-Controlled Key (CWE-639) in Kibana can lead to unauthorized cross-space access via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). The result is disclosure of inference output from a trained model in a different space that the user is not authorized to list, read, or use, which exposes the behavior of a model. The same pattern also reached the deployment stop and deployment update operations, allowing an active trained model deployment in another space to be stopped or to have its allocated resources altered.	2026-08-13	7.1	CVE-2026-72629
Elastic--Kibana	Incorrect Authorization (CWE-863) in Kibana Fleet can lead to privilege escalation via Privilege Abuse (CAPEC-122). Fleet restricts some callers to managing integration policies for one specific integration. When an existing integration policy was updated, that restriction was evaluated against the integration recorded on the stored policy rather than against the replacement integration supplied with the update. An authenticated user holding only the Elastic Defend endpoint policy management privilege was therefore able to convert an endpoint policy they administer into a policy for a different integration, and to supply that integration's configuration at the same time.	2026-08-13	7.1	CVE-2026-72630
Elastic--Kibana	Observable Discrepancy (CWE-203) in Kibana Fleet can lead to information disclosure via Excavation (CAPEC-116). Fleet removes the Elasticsearch API key value of an enrolled Elastic Agent from the responses of its agent listing capability, but that capability accepted caller-supplied filter expressions over the stored field that holds the value, and evaluated them with Kibana's own internal Elasticsearch privileges rather than the caller's. Because the number of matching agents is reported back to the caller, the difference between a matching and a non-matching filter formed a side channel from which the full API key value could be reconstructed one character at a time with a short sequence of requests.	2026-08-13	7.1	CVE-2026-72632
Elastic--Kibana	Kibana Agent Builder determines whether a caller owns a private agent by comparing a stable user identifier when one is recorded, and falling back to a comparison of the username when it is not. A username is not unique across Elasticsearch authentication realms, so two distinct principals that share a username in different realms are treated as the same owner. This discloses the configuration and instructions of an agent the caller does not own, and allows that agent to be altered or removed.	2026-08-13	7.1	CVE-2026-72643
Elastic--Kibana	Cross-Site Request Forgery (CWE-352) in Kibana can lead to privilege escalation via Cross Site Request Forgery (CAPEC-62). A user who is permitted to create visualizations can save a specially crafted Vega visualization that, when it is opened by another user, causes authenticated requests to be issued to Kibana in the context of the viewing user's session.	2026-08-13	7.3	CVE-2026-72658
Elastic--Kibana	The state that Kibana stores for an Observability Onboarding flow is not bound to the user who created the flow, and the routes that read and update that state do not verify ownership. An authenticated user who holds only generic read access to the space can therefore discover the onboarding flows of other users, read their onboarding state, and write arbitrary progress data into them. A tampered flow can also cause the owner's onboarding view to fail with a server error.	2026-08-13	7.6	CVE-2026-72669

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elastic--Kibana	A lower privileged user who holds only the privilege to read agent policies can read the entire configuration of a configured Fleet proxy. This would normally require the Fleet privilege to read settings. The proxy configuration possibly contains proxy authentication credentials and private key material that they should not be authorized to view.	2026-08-13	7.7	CVE-2026-72670
Elastic--Kibana	The Elastic Security capability that suggests existing field values while a user authors endpoint policy artifacts queries Elastic Defend event data with Kibana's internal Elasticsearch account instead of the account of the requesting user. Only Kibana feature privileges are verified, and the caller's Elasticsearch index privileges are not. An authenticated user who holds Elastic Security feature privileges but no read access to the Elastic Defend event indices can therefore retrieve field values from that data, including process command line arguments, which commonly contain tokens, credentials, connection strings, and other sensitive operational detail from protected hosts.	2026-08-13	7.7	CVE-2026-72672
Elastic--Kibana	Missing Authorization (CWE-862) in Kibana can lead to cross-space information disclosure and unauthorized data modification via Privilege Abuse (CAPEC-122). Kibana Machine Learning carries out its Elasticsearch operations with elevated internal permissions and relies on a per-request space filter to keep the machine learning data of one space separated from another. Part of the Machine Learning functionality did not apply that filter, so operations issued from one space were carried out against the machine learning data of every space in the deployment.	2026-08-13	7.1	CVE-2026-72675
Elastic--Kibana	Relative Path Traversal (CWE-23) in Kibana can lead to the unauthorized deletion of Kibana resources via Relative Path Traversal (CAPEC-139). Kibana Fleet accepted a user-supplied identifier for a Fleet Server host configuration without rejecting relative traversal sequences. The identifier is stored as provided and is later incorporated into the request that Kibana issues when that configuration is removed.	2026-08-13	7.3	CVE-2026-72677
electerm--electerm	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. Prior to 3.15.120, electerm allows a malicious SFTP server to write attacker-controlled content outside the temporary directory because the server-controlled filename name used by editWithSystemEditor in src/client/components/sftp/file-item.jsx is interpolated into path.resolve without sanitization. This issue is fixed in version 3.15.120.	2026-08-11	8.1	CVE-2026-73223
electerm--electerm	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. Prior to 3.15.120, electerm allows a malicious FTP or SFTP server to execute arbitrary commands when a user downloads a crafted folder and invokes Properties and Calculate Size because calcLocal in src/client/components/sftp/file-info-modal.jsx inserts the server-controlled folder name into a du -sh shell command without safely escaping single quotes. This issue is fixed in version 3.15.120.	2026-08-11	8.8	CVE-2026-73224
electerm--electerm	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. Prior to 3.15.120, electerm allows a malicious FTP or SFTP server to write attacker-controlled content outside the selected download directory because recursive transfers in src/client/components/file-transfer/transfer.jsx pass server-supplied file.name and folder.name values to resolve without sanitization. This issue is fixed in version 3.15.120.	2026-08-11	8.1	CVE-2026-73225
electerm--electerm	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. Prior to 3.15.186, electerm allows an authenticated WebSocket client to invoke unintended internal functions through client-controlled func values in upgrade-func in src/app/server/dispatch-center.js and handleFs in src/app/server/fs.js, exposing Upgrade and fsExport methods that can execute commands, open files, mutate the filesystem, or terminate the process. This issue is fixed in version 3.15.186.	2026-08-11	8.8	CVE-2026-73226
electerm--electerm	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. Prior to 3.15.120, electerm allows a malicious RDP server to write attacker-controlled content outside the selected save directory because the RDP clipboard download path in src/client/components/rdp/file-transfer.js passes the server-controlled CLIPDRD filename fileInfo.name to osResolve without sanitization. This issue is fixed in version 3.15.120.	2026-08-11	8.1	CVE-2026-73227
emlog--emlog	Emlog is an open source website building system. In 2.6.26 and earlier, install.php accepts action=reinstall without authentication and deliberately skips the already-	2026-08-14	9.8	CVE-2026-73849

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	installed check because the guard runs only when \$act != 'reinstall'. A remote attacker can submit hostname, dbuser, dbpasswd, dbname, dbprefix, username, password, and email values to cause file_put_contents('config.php', \$config) to overwrite the configuration with attacker-controlled database settings and create a new administrator account. No fixed version is available as of this review.			
eosphoros-ai--DB-GPT	DB-GPT v0.8.1 contains an unauthenticated path traversal vulnerability that allows remote attackers to write arbitrary files to any location on the server by injecting directory traversal sequences into the user_id HTTP header of the Python file-upload endpoint. Attackers can send a crafted multipart upload request with a traversal-poisoned user_id header to escape the intended upload directory and write attacker-controlled content to locations such as Python startup hooks, cron directories, or agent scripts, resulting in remote code execution.	2026-08-11	9.8	CVE-2026-73034
Essekia--Tablesome Table	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Essekia Tablesome Table allows Blind SQL Injection. This issue affects Tablesome Table: from n/a through 1.2.9.	2026-08-12	9.3	CVE-2026-66659
eteubert--Podlove Podcast Publisher	The Podlove Podcast Publisher plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the create_link_item function in all versions up to, and including, 4.5.3. This makes it possible for authenticated attackers, with contributor-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). A viable POP chain exists within the plugin itself via Podlove\ImageCache\GenerationGuard, whose __destruct() method invokes wp_delete_file() with an attacker-controlled file path populated through unserialization.	2026-08-16	8.8	CVE-2026-16099
Eugeny--tabby	Tabby (formerly Terminus) is a highly configurable terminal emulator. Prior to 1.0.235, a malicious SFTP server can return a backslash traversal filename through entry.name. In tabby-ssh/src/session/sftp.ts, SFTPSession.readdir() and _makeFile() use POSIX path processing that preserves the backslashes as ordinary filename characters. In tabby-ssh/src/components/sftpPanel.component.ts, downloadFolderRecursive() propagates item.name into the local relative path. In tabby-electron/src/services/platform.service.ts, ElectronDirectoryDownload.createFile() passes that path to Windows-native path.join(), and in tabby-electron/src/sftpContextMenu.ts, EditSFTPContextMenu.edit() passes item.name to path.join() for the temporary edit path. Windows interprets the preserved backslashes and parent-directory components as traversal, allowing attacker-controlled content to be created or overwritten outside the selected download directory or temporary edit directory. This issue is fixed in version 1.0.235.	2026-08-10	8.1	CVE-2026-72903
everestthemes--Everest Backup	Unauthenticated SQL Injection in Everest Backup <= 2.3.12 versions.	2026-08-13	9.3	CVE-2026-66472
Evergreen--Evergreen	A vulnerability has been found in Evergreen up to 3.14.11/3.15.11/3.16.5/3.17-beta1. The affected element is an unknown function of the file /osrf-gateway-v1 of the component open-ils.fielder OpenSRF Service. Such manipulation leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.14.12, 3.15.12, 3.16.6 and 3.17-beta2 is sufficient to fix this issue. The affected component should be upgraded.	2026-08-16	7.3	CVE-2026-19926
fahdaslam--Social Login, Passkeys, Magic Link & Email OTP Passwordless Login by VentraConnect	The Social Login, Passkeys, Magic Link & Email OTP - Passwordless Login by VentraConnect plugin for WordPress is vulnerable to Authentication Bypass via Unverified Provider Email in all versions up to, and including, 1.4.3. This is due to the plugin trusting the unverified email field returned by Spotify's /v1/me endpoint as proof of mailbox ownership - Generic::normalize_common() copies this value into the normalized profile without requiring an email_verified assertion, and User_Links::link_or_login_user() subsequently passes it directly to get_user_by('email', \$email) and issues a persistent authentication cookie via wp_set_auth_cookie() without a provider-specific verified-email gate, a local mailbox challenge, or a logged-in approval step. This makes it possible for unauthenticated attackers to log in as any existing WordPress user, including Administrators, by supplying a known target email address through a controlled Spotify OAuth flow, gaining full administrative access to the site.	2026-08-12	8.1	CVE-2026-18961
faker-js--faker	Faker generates massive amounts of fake data in the browser and Node.js. Prior to 10.5.0, the faker.helpers.fake method in src/modules/helpers/eval.ts allows attacker-controlled fake templates to access the Function constructor through	2026-08-11	7.8	CVE-2026-73231

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	fakeEval.resolveProperty when a function returns another function, enabling arbitrary JavaScript code execution. This issue is fixed in version 10.5.0.			
fashionstorage--Propovoice: All-in-One Client Management System	The Propovoice: All-in-One Client Management System plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.7.8. This is due to the `create()` function's REST endpoint failing to validate the user-supplied `role` parameter against an allowlist of permitted WordPress roles and omitting any `promote_users` capability check before passing the sanitized value directly to `WP_User::set_role()`. This makes it possible for authenticated attackers with `ndpv_manager`-level access and above to create a new WordPress user account with the `administrator` role assigned, achieving full vertical privilege escalation. The `ndpv_manager` capability is a sub-administrator CRM team role granted by Propovoice itself, meaning the attack surface extends beyond site administrators to any user the plugin has elevated to a manager position.	2026-08-15	8.8	CVE-2026-15312
fastschema--fastschema	A NULL pointer dereference vulnerability in fastschema through v0.15.1 allows an unauthenticated remote attacker to crash the server process with a single HTTP request. The sendOTPEmail function in pkg/auth/local.go dereferences a pointer obtained from an unchecked error path without validating it is non-nil, causing a fatal panic that terminates the entire server when a recovery request is sent to the /api/auth/local/recover endpoint.	2026-08-10	7.5	CVE-2026-72582
fastschema--fastschema	A time-of-check/time-of-use (TOCTOU) race condition in fastschema through v0.15.1 allows an unauthenticated remote attacker to bypass the OTP attempt limit on the account recovery flow, enabling brute-force attacks on 6-digit OTP codes.	2026-08-10	7.4	CVE-2026-72584
ffuf--ffuf	ffuf is a fast web fuzzer written in Go. Prior to 2.2.0, ffuf allows a malicious target server to cause an out-of-memory denial of service because the response size guard in pkg/runner/simple.go checks only the compressed Content-Length while io.ReadAll reads gzip, brotli, deflate, transparently decompressed, or chunked response bodies without a decompressed-size bound. This issue is fixed in version 2.2.0.	2026-08-11	7.5	CVE-2026-73232
filebrowser--filebrowser	filebrowser through 2.63.16 fails to properly restrict scope and permissions when self-signup is enabled with default CreateUserDir setting. Unauthenticated attackers can register accounts that inherit the server root scope with full create, modify, delete, rename, share, and download permissions, allowing unrestricted access to all files.	2026-08-13	9.8	CVE-2026-72839
filebrowser--filebrowser	FileBrowser before 2.63.19 does not account for case-insensitive filesystems when checking home directory ownership during self-registration. When Signup and CreateUserDir are enabled and FileBrowser's root is on a case-insensitive filesystem (confirmed on Windows/NTFS), two self-registered usernames that differ only in letter case (e.g., CaseVictim and casevictim) are stored as distinct accounts but resolve to the same physical home directory, because the scope-ownership check compares the persisted scope as an exact case-sensitive string. A second registrant can therefore read, overwrite, and delete another account's files through authenticated HTTP endpoints, without needing an existing account or victim interaction.	2026-08-14	8.1	CVE-2026-72836
filebrowser--filebrowser	File Browser versions before 2.63.20 fail to honor the createUserDir isolation in proxy and hook authentication auto-provisioning paths. Attackers with valid upstream-authenticated credentials can read, modify, delete, and share files belonging to other users by exploiting the server root scope assignment.	2026-08-14	8.8	CVE-2026-72837
filebrowser--filebrowser	File Browser before v2.63.22 fails to validate access rules for descendants during recursive copy, rename, and delete operations, allowing authenticated users to bypass path-based access controls. Attackers can copy, rename, or delete denied files by operating on their allowed parent directory, defeating rule-based isolation for confidentiality and integrity.	2026-08-13	8.1	CVE-2026-73612
filebrowser--filebrowser	filebrowser versions before 2.63.19 contain an out-of-scope file deletion vulnerability in the TUS upload cache eviction mechanism that allows authenticated users with only Create permission to delete arbitrary files outside their scope. Attackers can swap an ancestor directory with a symlink during the cache TTL window to redirect the raw os.Remove call to an out-of-scope target, bypassing ScopedFs scope guards and Perm.Delete checks.	2026-08-13	8.2	CVE-2026-73613
FileRun--FileRun	FileRun up to and including version 2026.2.0 contains an OS command injection vulnerability that allows authenticated attackers to achieve remote code execution by uploading a file with a malicious filename containing shell command substitution sequences. The thumbnail generation system passes filenames wrapped in shell double-quotes directly to exec() without escapeshellarg()	2026-08-11	8.8	CVE-2026-14863

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sanitization, allowing filenames such as \$(PAYLOAD).mp4 to survive the filename sanitizer and be evaluated as shell commands when ffmpeg, ImageMagick, vips, or stl-thumb processes the file during thumbnail generation.			
FitSoft--POS System	POS System developed by FitSoft has a Missing Authentication vulnerability. Unauthenticated remote attackers can directly access and operate the system.	2026-08-12	8.2	CVE-2026-19426
Flow Neuroscience--FL-100	An undocumented hard-coded credential, shared by all device units, is authorized to bypass authentication. This allows an attacker within Bluetooth range to arbitrarily manipulate brain stimulation parameters and state.	2026-08-13	8.1	CVE-2026-18164
FlowiseAI--Flowise	Flowise versions 2.2.4 through 3.1.4 contain a missing authorization vulnerability in the POST /api/v1/openai-assistants-file/download endpoint that allows unauthenticated attackers to access private files by exploiting the endpoint's inclusion in the global authentication whitelist, which bypasses all session and API key verification. Attackers can supply valid chatflowid, chatId, and fileName identifiers to retrieve files from any chatflow on the instance, including private chatflows belonging to other workspaces or organizations.	2026-08-10	7.5	CVE-2026-71962
FluxBuilder--MStore API	Unauthenticated Privilege Escalation in MStore API <= 4.20.0 versions.	2026-08-13	8.1	CVE-2026-27543
flytohub--flyto-core	Flyto2 Core before 2.28.0 contains a server-side request forgery guard bypass vulnerability that allows attackers to reach internal services by supplying URLs using the unblocked IPv6 address '::' which the kernel routes to loopback identically to '0.0.0.0'. Attackers can submit requests or trigger 302 redirects to ` to bypass the private IP range and blocked hostname checks in `is_private_ip()`, reaching services bound to IPv6 loopback across the `http.get`, `http.request`, and `http.batch` modules.	2026-08-13	7.7	CVE-2026-73530
Fortinet--FortiClientWindows	A buffer copy without checking size of input ('classic buffer overflow') vulnerability in Fortinet FortiClientWindows 7.4.0 through 7.4.3, FortiClientWindows 7.2.0 through 7.2.11 may allow an unauthenticated attacker in a position to alter or craft DNS responses to the targeted host to execute arbitrary code via malicious packets.	2026-08-12	7.3	CVE-2026-70465
Fortinet--FortiManager	A authentication bypass using an alternate path or channel vulnerability in Fortinet FortiManager 7.6.1, FortiManager 7.4.3 through 7.4.5, FortiManager 7.2.5 through 7.2.9, FortiManager Cloud 7.6.1, FortiManager Cloud 7.4.3 through 7.4.5, FortiManager Cloud 7.2.5 through 7.2.9 may allow attacker to improper access control via <insert attack vector here>	2026-08-12	7.3	CVE-2026-70468
Fortinet--FortiWeb	An Improper Authentication vulnerability [CWE-287] vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.2, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.0 through 7.4.11, FortiWeb 7.2.0 through 7.2.12, FortiWeb 7.0.0 through 7.0.12 may allow a remote unauthenticated attacker to login into the Fortiweb GUI/CLI with a random username and password	2026-08-12	8.8	CVE-2026-26035
Fosowl--AgenticSeek	AgenticSeek (commit fc242c7) contains an unauthenticated remote code execution vulnerability that allows any network-adjacent attacker to execute arbitrary commands by submitting crafted queries to the unprotected POST /query API endpoint bound to 0.0.0.0:7777 with wildcard CORS. Attackers can send unauthenticated HTTP requests that cause the autonomous agent to generate and execute shell commands through BashInterpreter using subprocess.Popen with shell=True and safety=False, bypassing the incomplete command blacklist to achieve full host-level code execution.	2026-08-13	9.8	CVE-2026-72776
fosrl--Pangolin	An improper authorization vulnerability in fosrl/pangolin through v1.20.0 allows an authenticated remote attacker to authenticate to any resource in any organization by reusing an access token issued for a different resource.	2026-08-10	9.6	CVE-2026-72564
frangoteam--FUXA	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. In fuxa-server version 1.3.0, the GET /api/project endpoint exposes sensitive project configuration data to guest-context requests even when secureEnabled is enabled. Version 1.3.1 fixes the issue.	2026-08-12	7.5	CVE-2026-47717
frangoteam--FUXA	A missing authentication vulnerability in frangoteam/FUXA through 1.3.3 allows an unauthenticated remote attacker to query all historical sensor data via the DAQ_QUERY Socket.IO event. When secureEnabled=true, all other sensitive Socket.IO events (DEVICE_BROWSE, HOST_INTERFACES, DEVICE_TAGS_REQUEST, etc.) call isSocketAdminAuthorized to verify the connection token, but the DAQ_QUERY handler in server/runtime/index.js lacks this check entirely.	2026-08-10	7.5	CVE-2026-72586
frappe--erpnext	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.118.0 and 16.29.0, the validate_template and render_template calls in erpnext/accounts/doctype/process_statement_of_accounts/process_statement_of_accounts.py render subject, body, and pdf_name fields with unrestricted globals	2026-08-10	9.9	CVE-2026-72911

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	including frappe.utils, allowing an authenticated user with a common operational role to inject template expressions, execute arbitrary server-side code, and read data across the application. This issue is fixed in versions 15.118.0 and 16.29.0.			
frappe--erpnext	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.112.0 and 16.22.0, the merge_account, pause_job_for_doc, trigger_job_for_doc, change_release_date, and update_cost_center functions across erpnext/accounts/doctype/account/account.py, erpnext/accounts/doctype/process_payment_reconciliation/process_payment_reconciliation.py, erpnext/accounts/doctype/purchase_invoice/purchase_invoice.py, and erpnext/accounts/utils.py omit required write permission checks, allowing authenticated limited users to modify protected data beyond their roles. This issue is fixed in versions 15.112.0 and 16.22.0.	2026-08-10	7.1	CVE-2026-72910
FreeCAD--FreeCAD	FreeCAD is a free and open-source multiplatform 3D parametric modeler. Prior to 1.1.2, PropertyFileIncluded::Restore() in src/App/PropertyFile.cpp concatenates an attacker-controlled file or data attribute from Document.xml with the document transient path without rejecting directory components, absolute paths, or parent traversal. A crafted .FCStd archive with a matching FileIncluded XML attribute and ZIP entry can therefore write attacker-controlled content to arbitrary locations accessible to the FreeCAD user, potentially enabling persistence, credential compromise, configuration replacement, or code execution. This issue is fixed in version 1.1.2.	2026-08-11	7.8	CVE-2026-73234
FreePBX--FreePBX Framework	A cross-site request forgery (CSRF) vulnerability in FreePBX Framework 17.0 allows an unauthenticated remote attacker to perform administrative actions on behalf of an authenticated administrator.	2026-08-10	8.8	CVE-2026-72578
Friendica--Friendica	An SQL injection vulnerability in Friendica through the 2026.08-dev branch allows unauthenticated remote attackers to execute arbitrary SQL statements via the photo-view order parameter. The parameter is concatenated unescaped into a SHOW COLUMNS query via a bare PDO::query() call, enabling stacked statement injection. An unauthenticated attacker can read, modify, or delete the entire database.	2026-08-11	9.8	CVE-2026-72550
frostming--unearth	unearth through 0.18.2, fixed in commit 6c78164, contains a path traversal vulnerability in the is_within_directory function that fails to normalize paths before validation, allowing ../ sequences to bypass directory containment checks. Attackers can supply malicious tar archives with symlink members or traversal sequences to write files to arbitrary filesystem locations accessible to the process.	2026-08-10	8.1	CVE-2026-73030
Fujitsu Research--OneCompression	Fujitsu Research's OneCompression library 1.2.0 contains an unsafe deserialization vulnerability that allows attackers to execute arbitrary code by supplying a crafted model.pt checkpoint file, as QuantizedModelLoader.load_quantized_model_pt() unconditionally calls torch.load with weights_only=False, invoking Python's pickle machinery during deserialization. Attackers can embed malicious __reduce__ methods in a crafted model checkpoint to execute arbitrary Python code, including system commands, when the library loads the file from a caller-selected model directory.	2026-08-12	7.8	CVE-2026-73325
gabehf--Koito	A server-side request forgery (SSRF) vulnerability in gabehf/Koito through v0.3.2 allows an authenticated user to make the server perform HTTP requests to arbitrary internal or external hosts by supplying a crafted image_url value in the PATCH /apis/web/v1/album/{id}/image endpoint.	2026-08-10	7.7	CVE-2026-72591
gamerz--WP-Stats	The WP-Stats plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.56 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-14	7.2	CVE-2026-19794
genkit-ai--genkit	Genkit does not properly validate host request headers. Any host on the developer's network, and any website the developer visits (via DNS rebinding), can reach POST /api/runAction on the Dev UI server (default port 4000) and execute any registered Genkit action and read the result. Fixed on 2026-06-18.	2026-08-11	7.8	CVE-2026-67179
getgrav--grav	The getgrav/grav-plugin-api Composer package before 1.0.13 (affected <= 1.0.12) fails to enforce API key scope caps on the disable2fa endpoint. Unlike the sibling generate2fa endpoint, disable2fa authorizes the admin (non-self) path solely via ACL reads (isSuperAdmin/hasPermission) and never invokes requirePermission(), so the api_key_scopes cap is never applied. As a result, a holder of a narrow-scope API key on a super account, or a non-super account whose ACL includes api.users.write, can force-disable two-factor authentication on any non-super target account via POST /api/v1/users/{user}/2fa/disable without providing a TOTP code, facilitating account takeover.	2026-08-14	9.8	CVE-2026-72822

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getgrav--grav	The Grav API plugin (getgrav/grav-plugin-api) before 1.0.13 contains an API key scope-cap bypass in PagesController::guardTwigContent(). The Twig-toggle check uses a bare isSuperAdmin() gate that does not consult api_key_scopes, so a least-privilege API key scoped only to api.pages.write and minted on a super account can enable process.twig on a page save even though admin.pages.twig is intentionally outside the api.pages scope. When security.twig_content.process_enabled=true and editor_enabled=false, this allows Twig-in-content to execute server-side, resulting in server-side template injection (SSTI) and remote code execution.	2026-08-14	9.8	CVE-2026-72824
getgrav--grav	The getgrav/grav-plugin-api plugin before 1.0.13 fails to validate that the scopes of a newly created API key are a subset of the caller's scopes in createApiKey. The self-target path of requireApiKeyPermission() requires only the baseline api.access scope, and the new key's scopes are read directly from the request body with no subset check. An attacker holding a minimal-scope API key on a super account can submit an empty scopes array to mint an unscoped, full-access super key, bypassing scope restrictions (and enabling further chains such as configuration write to RCE).	2026-08-14	9.8	CVE-2026-72826
getgrav--grav	The Grav API plugin (getgrav/grav-plugin-api) before 1.0.13 contains an API-key scope-cap bypass in UsersController's create() and update() methods. These methods enforce the scope cap only for api.users.write, but gate super-privilege grants on a bare isSuperAdmin() check that reads access.api.super directly without consulting the key's scopes. As a result, an api.users.write-scoped key minted on a super account can set access.api.super or assign a super-granting group to mint or promote a full super account, then authenticate as that account for uncapped administrative privileges.	2026-08-14	9.8	CVE-2026-72829
getgrav--grav	Grav API plugin versions before 1.0.13 fail to enforce API key scope caps in ConfigController super-scope gates, allowing scoped keys to write scheduler configuration. Attackers with a scoped api.config.write key can inject arbitrary commands into scheduler.custom_jobs that execute via Symfony Process for remote code execution.	2026-08-14	9.8	CVE-2026-72830
getgrav--grav	Grav CMS before 2.0.13 contains a remote code execution vulnerability in the Flex Objects plugin settings validation that allows authenticated users to execute arbitrary code by uploading a ZIP file containing PHP code. Attackers can bypass routine name validation by using array notation instead of string notation, call the unzip routine with a malicious archive, and write PHP files to the web root for execution.	2026-08-14	8.8	CVE-2026-72819
getgrav--grav	Grav CMS before 2.0.13 contains a server-side template injection vulnerability in email-action parameters that allows low-privileged page editors to execute arbitrary operating-system commands. Attackers can inject Twig payloads using the unsandboxed find filter in email subject, body, to, or from fields to achieve remote code execution when forms are submitted.	2026-08-14	8.8	CVE-2026-72827
getgrav--grav	The Flex Objects plugin (through 1.4.6, tested with Grav 2.0.11) contains an incorrect authorization vulnerability in its Flex Objects API. FlexApiController::update() checks only the general Flex directory permission and does not apply the additional target/field/super-admin checks enforced by the dedicated Users and Groups API controllers. An authenticated account with api.access, admin.login, and users.update permissions (but without api.users.write or admin.super) can use the generic /api/v1/flex-objects/user-accounts endpoint to change a super administrator's password, or the /api/v1/flex-objects/user-groups endpoint to grant its group admin.super, resulting in full site takeover. Fixed in Flex Objects 1.4.7.	2026-08-14	8.8	CVE-2026-72831
getgrav--grav	The Grav API plugin (getgrav/grav-plugin-api) versions >= 1.0.6 and <= 1.0.11 contain a privilege escalation vulnerability. A scoped API key minted on a super-admin account bypasses its declared scope cap on four isSuperAdmin()-gated write endpoints (in GroupsController, AccountsConfigController, PreferencesController, and DashboardWidgetController). These endpoints authorize via a super-admin early-return that never invokes requirePermission()-the sole enforcement point of the scope cap-so a 'read-only'-scoped key (e.g. api.pages.read) can perform super-only write operations, including rewriting group ACL maps to grant super-admin privileges to arbitrary accounts. A leaked or delegated read-only CI/monitoring key can therefore gain full super-admin write capability. Fixed in 1.0.13.	2026-08-14	8.8	CVE-2026-72833
getgrav--grav	The getgrav/grav-plugin-api plugin before 1.0.13 contains an API-key scope cap bypass in the POST /reports/twig-content/allowlist endpoint (ReportsController). The endpoint enforces requirePermission('api.config.write') followed by a bare isSuperAdmin() check instead of requireSuper(). Because isSuperAdmin() reads	2026-08-14	7.6	CVE-2026-72825

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access.api.super directly and never consults api_key_scopes, a least-privilege API key scoped to api.config.write minted on a super account passes the gate, allowing an attacker to append attacker-chosen tokens to the security.twig_sandbox allowlist (persisted to user/config/security.yaml). Widening the allowlist turns any subsequent Twig-in-content render into an SSTI/RCE sink.			
getgrav--grav	Grav Plugin API (getgrav/grav-plugin-api) before 1.0.13 fails to enforce API-key scope caps in InvitationsController. The strip-super and accept-groups decisions are gated on a bare isSuperAdmin() check rather than a scope-aware permission check, so a least-privilege API key (scoped to api.users.write) minted on a super account can create an invitation record containing super-admin access flags. When the invitation is accepted, those flags are written verbatim to the new account, resulting in privilege escalation to a fully controlled super account.	2026-08-14	7.2	CVE-2026-72828
getkin--kin-openapi	kin-openapi is a Go project for handling OpenAPI files. Prior to 0.144.0, ValidationHandler.Load() in openapi3filter/validation_handler.go silently replaces a nil AuthenticationFunc with NoopAuthenticationFunc, which returns nil without checking credentials. This substitution causes every OpenAPI security requirement to be satisfied for unauthenticated requests when an application relies on ValidationHandler as its enforcement middleware. The no-op callback prevents the fail-closed ErrAuthenticationServiceMissing path from being reached and forwards the request to protected handlers that may require an API key, OAuth token, or another security scheme. This issue is fixed in version 0.144.0.	2026-08-12	9.1	CVE-2026-73501
Ghost Foundation--Ghost	A broken access control vulnerability in Ghost Foundation Ghost 5.x allows authenticated Author-role users to delete posts owned by other users. The post model permissible() cascade is missing the branch that handles the combined isAuthor and isDestroy condition, causing the authorization check to fall through and permit the deletion. An attacker with an Author account can delete any post on the platform.	2026-08-11	8.1	CVE-2026-72596
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed cross-site scripting due to improper neutralization of user-controlled data rendered in pagination controls by an analytics dashboard component.	2026-08-12	8.7	CVE-2026-15216
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed cross-site scripting due to improper neutralization of user-controlled values rendered in table cell content by an analytics dashboard component.	2026-08-12	8.7	CVE-2026-15217
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 19.0 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user with developer-role permissions to execute CI/CD pipelines on a protected branch without the required push permissions due to improper authorization in pipeline reference validation.	2026-08-12	8.5	CVE-2026-15423
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.4 and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user to cause AI usage to be attributed to another namespace, due to improper authorization of identity information supplied in requests.	2026-08-12	8.5	CVE-2026-19228
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.4 and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user to modify project settings restricted to higher-privileged roles, due to missing authorization checks on a project update endpoint.	2026-08-12	7.1	CVE-2026-16494
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user with developer-role permissions to escalate privileges due to improper sanitization of HTML content rendered in a CI job modal.	2026-08-12	7.7	CVE-2026-16627
gitpython-developers--GitPython	GitPython before 3.1.57 fails to guard git option forwarding in IndexFile.checkout() and TagReference.create(), allowing attackers to pass unsafe options via kwargs. Attackers can use --prefix to overwrite arbitrary files with repository content or -F to read arbitrary files returned in-band.	2026-08-13	8.1	CVE-2026-73620
gitpython-developers--GitPython	GitPython versions before 3.1.54 contain an arbitrary file overwrite vulnerability in the Diffable.diff method that fails to validate git options passed through kwargs. Attackers can supply the --output argument via the other parameter or output kwarg to write patch content to attacker-chosen file paths at process privilege level.	2026-08-13	8.1	CVE-2026-73624

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitpython-developers--GitPython	GitPython versions before 3.1.54 contain a remote code execution vulnerability in the check_unsafe_options guard that can be bypassed by smuggling git options inside single-character kwarg values. Attackers can supply crafted option dictionaries to clone_from, fetch, pull, push, ls_remote, iter_commits, blame, or archive methods to execute arbitrary OS commands via the --upload-pack parameter.	2026-08-13	8.8	CVE-2026-73625
gitpython-developers--GitPython	GitPython before 3.1.55 fails to disable environment variable expansion in Remote.create() and Submodule.add() URL handling, allowing attackers to exfiltrate secrets by supplying URLs containing variable references. Attackers can craft URLs with environment variable tokens that are expanded into .git/config and .gitmodules, then transmitted to attacker-controlled hosts during fetch or pull operations.	2026-08-13	7.5	CVE-2026-73622
gitpython-developers--GitPython	GitPython before 3.1.54 contains an incomplete denylist in unsafe_git_clone_options that omits --template, allowing attackers to achieve arbitrary command execution during clone operations. Attackers can supply --template pointing to a directory containing malicious post-checkout hooks that execute when git clones the repository.	2026-08-13	7.5	CVE-2026-73623
goodrain--rainbond	Rainbond through 6.9.7 contains a broken access control vulnerability in the CheckToken function that allows authenticated attackers to access unauthorized enterprise resources by substituting another enterprise's tenant name in URL paths. Attackers can use any valid API token to bypass enterprise ID verification and access or modify another enterprise's services, plugins, environment variables, and certificates.	2026-08-13	8.1	CVE-2026-72741
Google--Turbinia	Google Turbinia allows arbitrary command execution via worker tasks. An attacker with privileges to submit a processing request or influence an evidence path/name obtains code execution on the worker fleet. Fixed on 2026-07-10.	2026-08-11	8.4	CVE-2026-67180
Grafana--Grafana MCP Server	A caller-supplied X-Grafana-URL request header controls the destination of mcp-grafana's outbound requests, and the grafana_api_request tool lets the caller also choose the HTTP method, path, and body. Because the destination is not restricted to the configured Grafana instance, a caller can direct requests at internal, loopback, and link-local network services (including metadata endpoints) and read the responses, resulting in server-side request forgery. The fix for CVE-2026-15583 prevented the configured service-account token from being sent to unintended destinations but did not restrict the destinations themselves.	2026-08-11	9.1	CVE-2026-19516
GramSearch--telegram-search	telegram-search contains a stored cross-site scripting vulnerability that allows remote attackers to execute arbitrary JavaScript in victims' browsers by sending crafted messages containing unsanitized HTML to a shared Telegram group. The highlightKeyword function in MessageList.vue passes raw message content directly to v-html without HTML escaping or sanitization, enabling stored, cross-user, zero-click execution of injected payloads such as image onerror handlers when victims browse or search messages.	2026-08-11	8.7	CVE-2026-73031
Haiwell--Haiwell IoT Cloud HMI Gateway	A critical OS command injection vulnerability has been identified in the Haiwell IoT Cloud HMI Gateway product. The vulnerability exists in the Net Check feature accessible via the /setting endpoint. The cmdPing Socket.io event fails to properly sanitize user-supplied input before passing it to the underlying operating system, allowing an attacker to inject and execute arbitrary OS commands with root privileges.	2026-08-14	10	CVE-2026-19188
Hakan Ozevin--WP BASE Booking	Unauthenticated Arbitrary Code Execution in WP BASE Booking <= 6.3.0 versions.	2026-08-13	10	CVE-2026-61962
harttle--liquidjs	LiquidJS is a Shopify/GitHub Pages compatible template engine. Prior to version 10.26.0, it is possible to execute arbitrary code with crafted templates. Version 10.26.0 patches the issue.	2026-08-11	10	CVE-2026-45618
HashiCorp--Tooling	Vault Secrets Operator 1.3.0 up to 1.4.1 is vulnerable to an arbitrary file read and credential exfiltration issue in the AppRole authentication configuration that may allow a tenant with limited Kubernetes RBAC permissions to read files from the operator pod's filesystem and transmit their contents to a tenant-controlled endpoint, potentially leading to privilege escalation within the cluster. This vulnerability (CVE-2026-8715) is fixed in Vault Secrets Operator 1.5.0.	2026-08-13	9.6	CVE-2026-8715
HashiCorp--Vault Enterprise	Vault Enterprise's identity entity batch-delete endpoint is vulnerable to a cross-namespace authorization bypass that may allow an authenticated caller in one namespace to permanently delete the storage backing of entities belonging to another namespace. This vulnerability (CVE-2026-14886) is fixed in Vault Enterprise 2.0.4, 1.21.9, 1.20.14 and 1.19.20.	2026-08-10	8.2	CVE-2026-14886

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Hassan Fakihi--iCARRY	Unauthenticated Sensitive Data Exposure in iCARRY <= 2.9 versions.	2026-08-13	7.5	CVE-2026-66463
Hongjing Century--e-HR	Hongjing e-HR contains an unauthenticated SQL injection vulnerability in the getSdutyTree servlet endpoint that allows remote unauthenticated attackers to access protected resources by supplying a path traversal sequence in the request URI to bypass the oauthservlet authentication filter. Attackers can inject UNION-based SQL payloads through the unsanitized codeitemid parameter into the underlying Microsoft SQL Server query to retrieve sensitive database contents including user credentials. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-07-30 (UTC).	2026-08-13	7.5	CVE-2024-58374
http4s--blaze	Http4s (http4s-blaze-server) is a minimal, idiomatic Scala interface for HTTP services. Prior to 0.23.18 and 1.0.0-M42, http4s-blaze-server aggregates fragments of an incoming WebSocket message with no limit on total size or fragment count. A client that completes a WebSocket handshake can send an unterminated fragmented message and drive unbounded heap growth in the server JVM, resulting in denial of service through OutOfMemoryError. Any http4s application serving WebSocket routes over BlazeServerBuilder is affected, no non-default configuration is required, and maxWebSocketBufferSize does not bound the aggregate because it bounds only individual frames. A single connection sending continuation frames that never set FIN forces the server to buffer every fragment until the heap is exhausted, terminating the JVM with OutOfMemoryError on the blaze selector thread. Small fragments amplify the cost through per-frame object overhead, so a modest volume of wire bytes is sufficient. This issue is fixed in versions 0.23.18 and 1.0.0-M42.	2026-08-12	7.5	CVE-2026-73493
http4s--blaze	blaze is a Scala library for building asynchronous pipelines, with a focus on network IO. Prior to 0.23.18 and 1.0.0-M42, blaze-server can merge HTTP/1.1 chunked-body trailer fields into Request.headers. Because trailer fields are attacker-controlled, an unauthenticated remote client can inject arbitrary header names and values, including X-Forwarded-For and internal authorization headers, that a fronting proxy sanitized from the request-header section, bypassing header-based trust decisions in the application. Any http4s application using BlazeServerBuilder over HTTP/1.1 whose routes or middleware trust proxy-set headers, including X-Forwarded-For, X-Real-IP, and X-Forwarded-Host, is affected. If a fronting proxy strips or normalizes those headers but forwards chunked bodies with trailers intact, an attacker can spoof client IP for allow-lists, rate limits, or auditing, forge the https scheme, or inject internal authorization headers. A promoted Connection: close trailer is also honored, allowing attacker-controlled termination of pooled backend connections. This issue is fixed in versions 0.23.18 and 1.0.0-M42.	2026-08-12	7.4	CVE-2026-73495
huggingface--accelerate	Hugging Face Accelerate through 1.14.0 contains a path traversal vulnerability in load_checkpoint_in_model and load_checkpoint_and_dispatch functions that fail to sanitize weight_map entries from sharded checkpoint indexes. Attackers can supply relative paths with ../ sequences or absolute paths to read arbitrary files, or point shard entries at named pipes to cause indefinite blocking and denial of service.	2026-08-10	7.1	CVE-2026-69112
IBM--Db2	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.5 is vulnerable to buffer overflow in the IXF IMPORT parser.	2026-08-12	8.4	CVE-2026-10534
IBM--Db2	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.5 is vulnerable to privilege escalation with a specially crafted query.	2026-08-12	8.2	CVE-2026-10543
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-12	9.8	CVE-2026-16956
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to write files to arbitrary locations due to path traversal.	2026-08-14	9.3	CVE-2026-17181
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to bypass authentication and obtain or alter sensitive information due to improper validation of request URI path segments.	2026-08-14	9.8	CVE-2026-17182
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to execute arbitrary code due to external control of file name or path.	2026-08-14	9.8	CVE-2026-17184
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to execute arbitrary CL commands due to improper neutralization of special elements in a command.	2026-08-14	9.9	CVE-2026-17186
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to obtain sensitive information due to external control of system configuration.	2026-08-14	8.3	CVE-2026-16708

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to bypass security restrictions due to improper authorization using user-supplied input.	2026-08-14	8.8	CVE-2026-16879
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to write arbitrary files due to improper limitation of a pathname to a restricted directory.	2026-08-14	8.2	CVE-2026-17081
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to cause a denial of service due to command injection.	2026-08-14	8.5	CVE-2026-17179
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to obtain sensitive information due to improper input validation.	2026-08-14	7.5	CVE-2026-16915
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to obtain sensitive information due to improper authentication enforcement.	2026-08-14	7.5	CVE-2026-17175
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to cause a denial of service due to uncontrolled recursion.	2026-08-14	7.5	CVE-2026-17177
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to obtain sensitive information due to improper limitation of a pathname to a restricted directory.	2026-08-14	7.5	CVE-2026-18554
IBM--Documentation Offline	IBM Documentation Offline 1.0.0 through 1.4.1 could allow a remote attacker to execute arbitrary code due to improper control of file paths.	2026-08-13	9.8	CVE-2026-17482
IBM--Documentation Offline	IBM Documentation Offline 1.0.0 through 1.4.1 could allow a remote attacker to execute arbitrary code due to improper output neutralization for logs.	2026-08-13	8.8	CVE-2026-17481
IBM--Documentation Offline	IBM Documentation Offline 1.0.0 through 1.4.1 could allow a remote attacker to read arbitrary files due to improper limitation of a pathname to a restricted directory.	2026-08-13	7.5	CVE-2026-17473
IBM--DOORS Next	IBM DOORS Next 7.0.3 through 7.0.3 Interim Fix 018 could allow an authenticated user to bypass security logic to perform unauthorized activities.	2026-08-12	10	CVE-2024-27253
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary code due to an uncontrolled search path element.	2026-08-12	9.9	CVE-2026-16860
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to execute arbitrary code due to a stack-based buffer overflow.	2026-08-12	9.8	CVE-2026-17083
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to execute arbitrary code due to an out-of-bounds write.	2026-08-12	9.8	CVE-2026-17218
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to escalate privileges due to improper authorization in the handling of high-authority threads.	2026-08-12	9.6	CVE-2026-17276
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary code due to an untrusted search path.	2026-08-13	8.8	CVE-2026-16674
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain unauthorized privileges due to improper privilege management.	2026-08-13	8.8	CVE-2026-16722
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service and potentially obtain sensitive information due to a stack-based buffer overflow.	2026-08-13	8.6	CVE-2026-16815
IBM--i	IBM i 7.6, and 7.5 could allow a local attacker to gain elevated privileges due to improper neutralization of special elements used in an OS command.	2026-08-12	8.8	CVE-2026-16856
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to access server resources with the privileges of an authenticated user due to improper authentication during NTLM session negotiation.	2026-08-13	8.1	CVE-2026-16867
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to the use of uninitialized memory during ASN.1 length processing.	2026-08-13	8.1	CVE-2026-16868
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary commands due to improper privilege management during monitor owner reassignment.	2026-08-12	8.1	CVE-2026-16904
IBM--i	IBM i 7.6, and 7.5 could allow a remote authenticated attacker to execute arbitrary commands with elevated privileges due to improper neutralization of special elements used in an OS command.	2026-08-12	8.8	CVE-2026-16906
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to gain unauthorized access to arbitrary objects due to a path traversal vulnerability.	2026-08-13	8.5	CVE-2026-16908
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to gain unauthorized access to system objects due to a time-of-check to time-of-use (TOCTOU) race condition involving symbolic links.	2026-08-13	8.5	CVE-2026-16967
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary code due to a heap-based buffer overflow.	2026-08-13	8.8	CVE-2026-16975

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to gain elevated privileges due to improper validation of the LANG environment variable.	2026-08-13	8.8	CVE-2026-16987
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to execute arbitrary code due to an out-of-bounds write.	2026-08-13	8.8	CVE-2026-17029
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to perform unauthorized operations and access sensitive information due to improper session management.	2026-08-13	8.1	CVE-2026-17045
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to bypass security restrictions due to improper validation of anti-CSRF tokens.	2026-08-13	8.1	CVE-2026-17069
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to gain elevated privileges due to improper validation of a client-supplied profile name.	2026-08-12	8.8	CVE-2026-17082
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to bypass security restrictions due to unsafe reflection.	2026-08-12	8.3	CVE-2026-17095
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to execute arbitrary code or obtain sensitive information due to improper authentication.	2026-08-13	8.3	CVE-2026-17101
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary commands and obtain sensitive information due to improper privilege management.	2026-08-12	8.8	CVE-2026-17110
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to bypass security restrictions due to improper validation of client-asserted identity.	2026-08-13	8.1	CVE-2026-17197
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	2026-08-13	8.1	CVE-2026-17206
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service and modify authentication metadata due to a buffer overflow.	2026-08-13	8.2	CVE-2026-17220
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary code due to a buffer overflow.	2026-08-13	8.8	CVE-2026-17223
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to a buffer overflow.	2026-08-13	8.2	CVE-2026-17272
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of shell metacharacters.	2026-08-12	8.8	CVE-2026-17417
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local authenticated attacker to cause a denial of service due to improper neutralization of special elements used in an SQL command.	2026-08-12	8.5	CVE-2026-17418
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to bypass security restrictions due to improper validation of an attacker-supplied user profile name.	2026-08-12	8.2	CVE-2026-17445
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service and obtain sensitive information due to an integer underflow.	2026-08-12	8.2	CVE-2026-17485
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to an out-of-bounds write.	2026-08-13	8.6	CVE-2026-17502
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-12	8.8	CVE-2026-17642
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information and compromise system integrity due to an XML injection flaw.	2026-08-12	8.1	CVE-2026-18098
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary script code due to improper neutralization of user-controlled input.	2026-08-12	8.9	CVE-2026-18099
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to gain elevated privileges due to improper management of thread authority swaps.	2026-08-13	8.8	CVE-2026-18101
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to bypass security restrictions due to improper validation of user-controlled addresses.	2026-08-13	8.9	CVE-2026-18193
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary Control Language commands due to insufficient input validation.	2026-08-12	8.3	CVE-2026-18235
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to gain elevated privileges due to improper validation of pointers read from Java-controlled addresses.	2026-08-13	8.4	CVE-2026-18249
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local authenticated attacker to gain privilege escalation via the Navigator for i debugger. This could allow the attacker to access or manipulate sensitive data on the system, or create new profiles with elevated privileges on the IBM i system.	2026-08-13	8.2	CVE-2026-18509

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 is vulnerable to a privilege escalation as the result of a remote code execution vulnerability in the activation engine component. An authenticated attacker can execute a maliciously planted script with root authority.	2026-08-12	8.8	CVE-2026-18669
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 is vulnerable to privilege escalation via Navigator for i. An authenticated user could elevate privileges to a root user to execute commands.	2026-08-12	8.8	CVE-2026-18683
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 s vulnerable to privilege escalation via Navigator for i. An authenticated user could elevate privileges to a root user to execute commands.	2026-08-12	8.8	CVE-2026-18713
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote unauthenticated attacker to harvest credentials due to spoofing of Navigator for i.	2026-08-12	8.8	CVE-2026-18847
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to an out-of-bounds read.	2026-08-12	7.7	CVE-2026-16863
IBM--i	IBM i 7.6 could allow a remote attacker to cause a denial of service due to an out-of-bounds write.	2026-08-13	7.5	CVE-2026-16887
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local authenticated attacker to obtain unauthorized access to files due to a time-of-check time-of-use (TOCTOU) race condition.	2026-08-13	7.1	CVE-2026-16896
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local authenticated attacker to change the ownership of arbitrary files due to improper validation of an attacker-controlled file path.	2026-08-13	7.8	CVE-2026-16898
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary code due to improper bounds checking.	2026-08-12	7.6	CVE-2026-16907
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to improper handling of zero-length TCP options.	2026-08-12	7.5	CVE-2026-16931
IBM--i	IBM i 7.6, 7.5, and 7.4 s vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2026-08-13	7.6	CVE-2026-16961
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to a heap buffer overflow.	2026-08-13	7.5	CVE-2026-16982
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to an infinite loop.	2026-08-13	7.5	CVE-2026-17004
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to obtain sensitive information due to improper authentication.	2026-08-13	7.3	CVE-2026-17099
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 s vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2026-08-12	7.6	CVE-2026-17111
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to unbounded resource allocation.	2026-08-13	7.5	CVE-2026-17199
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to an infinite loop.	2026-08-13	7.5	CVE-2026-17229
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to cause a denial of service due to improper neutralization of special elements in an OS command.	2026-08-12	7.1	CVE-2026-17248
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to improper validation of input size.	2026-08-12	7.5	CVE-2026-17271
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to gain elevated privileges due to improper privilege management.	2026-08-13	7.8	CVE-2026-18071
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to a stack-based buffer overflow.	2026-08-13	7.5	CVE-2026-18077
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local authenticated attacker to generate a stack-based buffer overflow in the Native IBM i JSSE provider, caused by improper bounds checking during TLS session establishment. A local attacker could overflow a fixed-length buffer and execute arbitrary code on the system or cause the JVM process to crash.	2026-08-13	7.3	CVE-2026-18511
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 s vulnerable to a buffer overflow from improperly validating client data. By sending malformed requests to one of the host servers, a remote attacker could leverage this vulnerability to cause a denial-of-server (DoS) for that server.	2026-08-13	7.5	CVE-2026-18846
IBM--i Access Client Solutions	IBM i Access Client Solutions 1.1.2.0 through 1.1.9.13 is vulnerable to zip slip path traversal exploit when importing a configuration.	2026-08-12	8.8	CVE-2026-13105
IBM--i Access Client Solutions	IBM i Access Client Solutions 1.1.2.0 through 1.1.9.13 (ACS) is vulnerable to downloading unverified product code when configured to update from an IBM i. A	2026-08-12	8.3	CVE-2026-13433

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bad actor could use this vulnerability to run compromised code on the ACS user's workstation.			
IBM--i Access Client Solutions	IBM i Access Client Solutions 1.1.2.0 through 1.1.9.13 is vulnerable to arbitrary code execution on Windows when installed for all users due to publicly writeable configuration file.	2026-08-12	7.8	CVE-2026-13094
IBM--i Access Client Solutions	IBM i Access Client Solutions 1.1.2.0 through 1.1.9.13 is vulnerable to injection of rogue certificate authority due to publicly writeable truststore.	2026-08-12	7.7	CVE-2026-14866
IBM--i Access Client Solutions	IBM i Access Client Solutions 1.1.2.0 through 1.1.9.13 is vulnerable to arbitrary code execution on Windows when installed for all users due to publicly writeable directory.	2026-08-13	7.3	CVE-2026-14875
IBM--i Access Client Solutions	IBM i Access Client Solutions 1.1.2.0 through 1.1.9.13 could allow a local attacker to execute arbitrary code due to improper neutralization of special elements used in an OS command.	2026-08-12	7.8	CVE-2026-16695
IBM--Informix Dynamic Server	IBM Informix oninit sq_sgkprepare RCE via unchecked SQL Interface length field.	2026-08-12	8.8	CVE-2026-13361
IBM--Informix Dynamic Server	IBM Informix Dynamic Server 14.10, and 15.0 contain a local privilege escalation vulnerability in the oninit setuid-root utility.	2026-08-12	7.8	CVE-2026-13367
IBM--Informix Dynamic Server	IBM Informix Dynamic Server 14.10, 15.0, and 12.10 could allow an unauthenticated user to execute arbitrary commands with service account privileges on the system due to improper validation of user supplied input.	2026-08-12	7.3	CVE-2026-13476
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.6 could allow a remote attacker to obtain unauthorized access to user accounts due to improper restriction of excessive authentication attempts.	2026-08-13	9.1	CVE-2026-19297
IBM--Planning Analytics	IBM Planning Analytics 2.0, and 2.1 Local is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2026-08-13	7.1	CVE-2026-13365
IBM--Security Verify Access	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 and IBM Verify Identity Access Container 11.0 through 11.0.3 contains a format string injection vulnerability in the management interface that allows attackers to cause denial of service and information disclosure by crafting a malicious HTTP request.	2026-08-12	8.7	CVE-2026-12004
IBM--Security Verify Access	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 and IBM Verify Identity Access Container 11.0 through 11.0.3 could allow a remote attacker to access sensitive information due to an inconsistent interpretation of an HTTP request by a reverse proxy.	2026-08-12	8.1	CVE-2026-12359
IBM--Security Verify Access	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 and IBM Verify Identity Access Container 11.0 through 11.0.3 could allow an authenticated user to gain privileges of another user via a specially crafted request.	2026-08-12	8.1	CVE-2026-13267
IBM--Security Verify Access	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 and IBM Verify Identity Access Container 11.0 through 11.0.3 Reverse Proxy in certain configurations may provide weaker than expected cryptographic validation of user supplied data.	2026-08-12	7.4	CVE-2026-11923
IBM--Security Verify Access	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 and IBM Verify Identity Access Container 11.0 through 11.0.3 contains a input validation vulnerability in the management interface that allows already privileged attackers to execute additional operations by crafting a malicious HTTP request.	2026-08-12	7.2	CVE-2026-12005
IBM--Security Verify Access	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 and IBM Verify Identity Access Container 11.0 through 11.0.3 could allow an administrator to execute additional commands they are not entitled to due to improper validation of user supplied input.	2026-08-12	7.2	CVE-2026-12618
IBM--Storage Scale	IBM Storage Scale 5.2.3.0 through 5.2.3.8, and 6.0.0.0 through 6.0.1.0 GUI contains a hardcoded token in the source code, which was used for inter-node cluster communication and REST API authentication between GUI.	2026-08-13	7.5	CVE-2026-13460
IBM--Storage Scale	IBM Storage Scale 5.2.3.0 through 5.2.3.8, and 6.0.0.0 through 6.0.1.0 Secrets may be disclosed in log files in IBM Storage Scale Management GUI The admin password is logged into the GUI log of IBM Storage Scale Systems Deploy and Upgrade from GUI. Secrets may be disclosed in information related to exceptions in IBM Storage Scale Management GUI.	2026-08-13	7.1	CVE-2026-19483
IBM--WebSphere Application Server - Liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 IBM WebSphere Application Server Liberty is vulnerable to an authentication bypass when the rtcomm-1.0 or rtcommGateway-1.0 feature is enabled.	2026-08-13	9.4	CVE-2026-14525

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--WebSphere Application Server - Liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is vulnerable to a privilege escalation when using Liberty collectives.	2026-08-12	8.1	CVE-2026-18499
Idurar--IDURAR ERP CRM	A broken access control vulnerability in Idurar IDURAR ERP CRM 4.1.0 allows unauthenticated remote attackers to download invoice PDF files containing customer PII via the /download router. The router is mounted without authentication middleware, making it publicly accessible. An attacker can enumerate MongoDB ObjectIds to download any invoice in the system without credentials.	2026-08-11	7.5	CVE-2026-72600
If-So Dynamic Content--If-So Dynamic Content Personalization	Subscriber SQL Injection in If-So Dynamic Content Personalization <= 1.10 versions.	2026-08-13	9.3	CVE-2026-66446
ImpressCMS--ImpressCMS	ImpressCMS contains an authenticated remote code execution vulnerability in the custom tag module that allows authenticated administrators to execute arbitrary PHP code by storing a malicious payload in a custom tag with PHP type enabled. The application decodes HTML-encoded content via undoHtmlSpecialChars() before passing it to eval() in the renderWithPhp() method, bypassing HTML Purifier sanitization, and the payload is triggered on every frontend page load through the preload event system.	2026-08-14	7.2	CVE-2026-73679
Imran Tauqeer--CubeWP	Subscriber SQL Injection in CubeWP <= 1.1.30 versions.	2026-08-13	8.5	CVE-2026-28168
infility--Infility Global	The Infility Global plugin for WordPress is vulnerable to Stored Cross-Site Scripting via /cf7_record Log Endpoint in all versions up to, and including, 2.15.21 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The /cf7_records viewer is accessible to any authenticated user including those with Subscriber-level access, meaning the injected payload executes for any logged-in user who visits the records page.	2026-08-16	7.2	CVE-2026-10734
instawp--InstaWP Connect 1-click WP Staging & Migration	The InstaWP Connect - 1-click WP Staging & Migration plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 0.1.3.6 via the (top-level script) function. This is due to the plugin stores its encrypted options file as options-{migrate_key}.txt in wp-content/instawpbackups/ without deploying an index.php or .htaccess to prevent directory listing, exposing the 40-character migrate_key on Apache servers with directory indexing enabled, which allows an attacker to derive the AES-256-CBC passphrase via SHA256(migrate_key), decrypt the options file to recover the api_signature. This makes it possible for unauthenticated attackers to get the database access details and api_signature. Exploitation requires the target WordPress site to be hosted on Apache with directory listing enabled (Options +Indexes) for the wp-content/instawpbackups/ directory, and time limited because it can only be exploited during the migration period.	2026-08-11	7.5	CVE-2026-13457
Insyde Software--InsydeH2O	In an UEFI, Lack of verified boot to certain FV may cause arbitrary code execution.	2026-08-12	8.2	CVE-2026-6484
Inventec Appliances--Chiline Cloud	Chiline Cloud developed by Inventec Appliances has a Insecure Direct Object Reference vulnerability. Unauthenticated remote attackers can modify a specific parameter to read other users' sensitive data.	2026-08-11	7.5	CVE-2026-19424
isaacs--node-tar	node-tar is a tar archive manipulation library for Node.js. Prior to 7.5.21, node-tar's filesFilter in src/list.ts uses the recursive mapHas helper to walk an archive entry path upward with path.dirname() and no segment cap when tar.t(...) or tar.x(...) receives a non-empty member-selection list. A crafted GNU L or PAX x long-path header with thousands of slash-separated segments reaches this.filter(entry.path, entry) in Parser[CONSUMEHEADER] in src/parse.ts before Unpack[CHECKPATH] applies maxDepth, causing an uncatchable RangeError stack overflow that terminates asynchronous and streaming Node.js consumers. This issue is fixed in version 7.5.21.	2026-08-13	7.5	CVE-2026-73566
Ishankjha740--ishankportfolio	ishankportfolio is a portfolio website. Prior to version 1.0.1, contact form submissions could potentially be exposed due to improperly secured client-side database configuration and insufficient access control policies. Applications using publicly exposed database credentials or permissive database rules may allow unauthorised users to read, modify, or abuse stored form submission data. This could impact personally identifiable information (PII) submitted through the website contact form, including names, email addresses, phone numbers, and messages. The issue has been patched in version 1.0.1. Users unable to upgrade	2026-08-11	8.2	CVE-2026-48771

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	immediately can reduce risk by disabling public read/write database access, rotating exposed API keys, restricting database policies to authenticated requests only, moving sensitive operations to secure backend/serverless functions, and/or monitoring database activity logs for suspicious access.			
Ivanti--Endpoint Manager	Cleartext transmission of sensitive information in the Core of Ivanti Endpoint Manager before version 2024 SU7 allows a remote unauthenticated attacker in a MITM position to leak credentials for external SQL connections.	2026-08-11	8.1	CVE-2026-18129
Ivanti--Endpoint Manager	An out-of-bounds read in the Agent of Ivanti Endpoint Manager before version 2024 SU7 allows a remote unauthenticated attacker to crash an agent service.	2026-08-11	7.5	CVE-2026-18125
Ivanti--Endpoint Manager	External control of a filename in the Core of Ivanti Endpoint Manager before version 2024 SU7 allows a remote authenticated attacker full write control over an S3 bucket configured for session recording storage.	2026-08-11	7.7	CVE-2026-18127
jackdewey--Link Library	The Link Library plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the ll_delete_link_fields function in all versions up to, and including, 7.9.4 This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). Exploitation requires the administrator to have enabled the 'Delete local file on link deletion' plugin option (disabled by default) and to subsequently permanently delete the attacker-submitted link, which is a routine moderation action.	2026-08-15	9.1	CVE-2026-18855
JanDeDobbeleer--oh-my-posh	Oh My Posh is the most customisable and low-latency cross platform/shell prompt renderer. Prior to 29.35.1, the setStyle() function in src/segments/path.go passed pt.Path, which includes raw folder names, to template.Render, whose function map exposes cmd, so an attacker-controlled directory name containing a Go template expression could execute arbitrary operating system commands as the current user whenever the prompt rendered inside that directory or a descendant. This issue is fixed in version 29.35.1.	2026-08-13	7.8	CVE-2026-73505
Jegstudio--Gutenverse Companion	Unauthenticated Server Side Request Forgery (SSRF) in Gutenverse Companion <= 2.5.1 versions.	2026-08-13	7.2	CVE-2026-66704
jfrog--artifactory	A low-privilege authenticated user may permanently remove protected internal metadata across repositories under specific conditions.	2026-08-12	8.1	CVE-2026-66375
jfrog--artifactory	An unauthenticated attacker may cause untrusted package content to be cached under specific conditions, potentially affecting artifact integrity and availability.	2026-08-12	8.1	CVE-2026-69105
jfrog--artifactory	A low-privileged user may poison cached artifact metadata under specific conditions, potentially causing consumers to retrieve untrusted content.	2026-08-12	8.8	CVE-2026-69106
jfrog--artifactory	JFrog Artifactory could return an internal anonymous-user token to an unauthenticated caller when anonymous access is disabled, potentially exposing sensitive resources.	2026-08-12	7.5	CVE-2026-42018
jfrog--artifactory	A Project Resource Manager may gain broader administrative privileges under specific conditions.	2026-08-12	7.2	CVE-2026-68752
jfrog--artifactory	A user with access to a valid SAML response may impersonate another user under specific conditions.	2026-08-12	7.5	CVE-2026-68757
jfrog--artifactory	A holder of a valid integration credential may impersonate other users under specific conditions.	2026-08-12	7.2	CVE-2026-68759
Jinher--OA	A weakness has been identified in Jinher OA 1.0. Impacted is an unknown function of the file /C6/JHSoft.Web.HrmAttendance/attendance_out_approve.aspx. This manipulation of the argument httpOID causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-15	7.3	CVE-2026-19905
Joomla--Joomla! CMS	Joomla 6.1.1 contains a path traversal vulnerability in the com_joomlaupdate extension that allows a Super User to be induced into extracting a crafted archive containing directory traversal sequences or absolute paths in ZIP entry filenames. Attackers can supply malicious ZIP entry names with parent-directory segments or absolute paths to the extract.php extraction routine, causing files to be written outside the intended destination root and enabling persistent remote code execution via planted PHP files.	2026-08-12	7.6	CVE-2026-73327
Jovancoding--Network-AI	Network-AI ClaudeHookBridge before 5.15.1 truncates the target string to 500 characters before evaluating denyPatterns, while Claude Code executes the full untruncated command. Attackers can position dangerous content past byte 500 in a Bash command field to bypass the operator's hard-deny list and execute arbitrary commands.	2026-08-13	8.8	CVE-2026-73614

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Jovancoding--Network-AI	Network-AI versions before 5.15.1 contain a security matcher bypass vulnerability where SandboxPolicy evaluates raw command strings with quotes preserved while the executor tokenizes commands by stripping quotes before execution. Attackers can craft quoted commands that evade blacklist checks and approval gates while the executor runs the identical unquoted dangerous argv.	2026-08-13	8.8	CVE-2026-73615
JuneAndGreen--sm-crypto	sm-crypto provides JavaScript implementations of the Chinese cryptographic algorithms SM2, SM3, and SM4. Prior to 0.5.0, the default no-argument sm2.generateKeyPairHex() path in Node.js uses the module-wide SecureRandom instance in src/sm2/utls.js, supplied by jsbn@1.1.0, which seeds an ARC4 stream from Math.random() and new Date().getTime() because window.crypto.getRandomValues is unavailable even though globalThis.crypto exists. An attacker who can observe the process's Math.random() outputs and estimate the key-generation time can reconstruct the seed, recover generated SM2 private keys, and predict signing ephemeral scalars used to forge signatures. This issue is fixed in version 0.5.0.	2026-08-13	9.1	CVE-2026-73567
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 2.0.0, Kestra's core/src/main/java/io/kestra/core/runners/pebble/functions/HttpFunction.java passes the user-controlled http() uri argument to URI.create() and the server-side HTTP client without restricting private, loopback, or link-local destinations, allowing an unauthenticated attacker to import and execute a flow that accesses internal services or cloud metadata.	2026-08-11	8.6	CVE-2026-73247
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 2.0.0-rc6, Kestra's worker/src/main/java/io/kestra/worker/endpoint/WorkerEndpoint.java serves GET /worker without authentication and serializes the complete live Task object, which can expose commands, environment variables, HTTP headers, connection details, plaintext credentials, and execution identifiers while the main API on port 8080 remains protected. This issue is fixed in 2.0.0-rc6.	2026-08-11	7.5	CVE-2026-73246
kilbot--WCPOS Point of Sale (POS) plugin for WooCommerce	The WCPOS - Point of Sale (POS) plugin for WooCommerce plugin for WordPress is vulnerable to Code Injection via the 'thermal' Template Engine in all versions up to, and including, 1.9.14 due to the Receipt_Renderer_Factory dispatching templates with the 'thermal' engine to the Legacy_Php_Renderer instead of a safe thermal-specific renderer. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to inject arbitrary PHP code into a template post that is subsequently written to a temporary file and executed via PHP's include(), resulting in remote code execution on the server. This requires the attacker to have Shop Manager-level access or above, as the template save path enforces a wcpes_template_settings nonce and the manage_woocommerce_pos capability check.	2026-08-16	7.2	CVE-2026-17581
Kingston--FURY CTRL RGB Control Software	A security flaw has been discovered in Kingston FURY CTRL RGB Control Software 2.0.65.0. The impacted element is an unknown function in the library NTIOLib_KSFX.sys of the component Driver. Performing a manipulation results in improper privilege management. The attack needs to be approached locally. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-10	7.8	CVE-2026-19381
Kitae Park--Mang Board WP	Unauthenticated Cross Site Scripting (XSS) in Mang Board WP <= 2.3.4 versions.	2026-08-13	7.1	CVE-2026-61974
Koha Community--Koha	A stored SQL injection vulnerability in Koha through 24.11.17, 25.05.12, 25.11.06, and 26.05.01 allows authenticated staff with the tools => items_batchmod permission to read arbitrary database contents by storing a SQL payload in the agefield value of an automatic item modification rule. The agefield value is stored verbatim to the system preference and later interpolated without parameterization into a SQL query in C4::Items::ToggleNewStatus (line 1228) when the scheduled cron job executes. The injection is SELECT-only under standard MariaDB/MySQL DBI single-statement execution; a time-based SLEEP payload is also achievable via the cron trigger. An attacker can read the entire Koha database including patron PII and staff bcrypt password hashes.	2026-08-11	7.1	CVE-2026-72607
Koha Community--Koha	An SQL injection vulnerability in Koha through 24.11.17, 25.05.12, 25.11.06, and 26.05.01 allows authenticated staff with the acquisition => order_receive permission to read arbitrary database contents via the orderby request parameter in acqui/parcels.pl. The parameter is passed to C4::Acquisition::GetInvoices, which allow-lists the column name but concatenates the direction token raw into the SQL ORDER BY clause without validation. Exploitation is blind (time-based) in	2026-08-11	7.1	CVE-2026-72609

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	production and allows extraction of patron PII, staff bcrypt password hashes, and two-factor secrets.			
kovidgoyal--calibre	calibre is an e-book manager. Prior to 9.12.0, the calibre Content Server endpoint POST /book-update-annotations/{library_id}/{book_id}/{fmt} in src/calibre/srv/books.py omits needs_db_write=True, causing Router.dispatch() to skip ctx.check_for_write_access() before update_annotations() passes attacker-controlled JSON to db.merge_annotations_for_book(), which allows a readonly user or an anonymous user on an unauthenticated deployment to persist unauthorized book annotation changes. This issue is fixed in version 9.12.0.	2026-08-11	7.5	CVE-2026-73249
ladela--Online Scheduling and Appointment Booking System Bookly	The Online Scheduling and Appointment Booking System - Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via bookly_speed_up_update_addons AJAX action in all versions up to, and including, 27.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injection point is the bookly_speed_up_update_addons AJAX action, which is registered as wp_ajax_nopriv_* and therefore reachable without authentication; the payload is stored verbatim in the bookly_log.details column when a request is submitted without a valid signature, and executes when an administrator later views the Diagnostics â†’ Logs page.	2026-08-16	7.2	CVE-2026-13424
Laravel--Socialite	Laravel Socialite's Facebook provider contains an authentication bypass vulnerability that allows unauthenticated attackers to replay captured OIDC id_tokens by exploiting the missing nonce claim validation in the getUserByOIDCToken() function within FacebookProvider.php. Attackers who obtain a valid, unexpired id_token issued for the same Facebook App ID can submit the captured token to the backend issuerFromToken() endpoint, bypassing authentication controls because signature, aud, and iss checks pass while no session-bound nonce comparison is performed, resulting in unauthorized access to victim accounts.	2026-08-14	8.1	CVE-2026-73683
Lasso Analytics, Inc.--Do Lasso	Subscriber SQL Injection in Do Lasso <= 358 versions.	2026-08-13	8.5	CVE-2026-28156
Lasso Analytics, Inc.--Do Lasso	Subscriber Path Traversal in Do Lasso <= 358 versions.	2026-08-13	7.5	CVE-2026-28157
Lasso Analytics, Inc.--Do Lasso	Unauthenticated Cross Site Scripting (XSS) in Do Lasso <= 358 versions.	2026-08-13	7.1	CVE-2026-28158
LB-LINK--X-PRO	A vulnerability was identified in LB-LINK X-PRO 1.0.22-20231206. The impacted element is an unknown function of the file /etc/shadow. The manipulation leads to hard-coded credentials. It is possible to initiate the attack remotely. A high degree of complexity is needed for the attack. The exploitability is regarded as difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-15	8.1	CVE-2026-19900
LB-LINK--X-PRO	A security flaw has been discovered in LB-LINK X-PRO 1.0.22-20231206. This affects an unknown function of the file /etc/config/easycwmp. The manipulation results in hard-coded credentials. It is possible to launch the attack remotely. Attacks of this nature are highly complex. The exploitability is reported as difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-15	8.1	CVE-2026-19901
Lenovo--Accessories and Display Manager	During an internal security assessment, a potential vulnerability was discovered in Lenovo Accessories and Display Manager for Enterprise for Windows that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-08-13	7.8	CVE-2026-63423
Lenovo--Commercial Vantage	During an internal security assessment, an improper link following vulnerability was identified in Lenovo Vantage and Lenovo Commercial Vantage that could allow a local authenticated user to execute code with elevated privileges.	2026-08-13	7	CVE-2026-15994
Lenovo--Dock Manager	During an internal security assessment, an improperly protected key was discovered in Lenovo Dock Manager that could allow a local authenticated user to escalate privileges.	2026-08-13	7.3	CVE-2026-63424
Lenovo--Dock Manager	During an internal security assessment, a potential improper permissions vulnerability was discovered in Lenovo Dock Manager that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-08-13	7.8	CVE-2026-63425
Lenovo--Dock Manager	During an internal security assessment, a potential vulnerability was discovered in Lenovo Dock Manager that could allow an authenticated local user to perform an arbitrary file deletion with elevated privileges.	2026-08-13	7.1	CVE-2026-63426

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Lenovo--System Update	A potential authentication bypass vulnerability was reported in Lenovo System Update that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-08-13	7	CVE-2026-6387
Lenovo--Vantage	An improper link following vulnerability was reported in the VantageCoreAddin for Lenovo Vantage and Lenovo Commercial Vantage that could allow a local authenticated user to perform an arbitrary file deletion with elevated privileges.	2026-08-13	7.1	CVE-2026-12036
Lester Chan--WP-Stats	Unauthenticated Cross Site Scripting (XSS) in WP-Stats <= 2.56 versions.	2026-08-13	7.1	CVE-2026-66426
libgit2--libgit2	libgit2 versions v0.27.0 through v1.9.0 built with the libssh2 SSH backend (USE_SSH=libssh2) contain a shell command injection vulnerability that allows remote attackers to execute arbitrary commands on an SSH server by supplying a repository path containing unescaped shell metacharacters such as single quotes, semicolons, or pipes. The gen_proto() function in ssh_libssh2.c inserts the repository path directly into a shell command string without escaping special characters before passing it to libssh2_channel_exec(), enabling an attacker to craft a malicious submodule URL in a .gitmodules file that, when processed during a recursive clone, causes the remote server's shell to interpret injected commands under the victim's SSH user account.	2026-08-11	9.6	CVE-2026-5917
libp2p--py-libp2p	py-libp2p is the Python implementation of the libp2p networking stack. In 0.7.0 and earlier, the yamux handle_incoming() method in libp2p/stream_muxer/yamux/yamux.py reads an attacker-controlled 32-bit DATA frame length with read_exactly() before validating it against MAX_WINDOW_SIZE or checking whether stream_id exists. A peer that completes the standard Noise handshake can send a 12-byte frame declaring a 0xFFFFFFFF body and then withhold the body, causing the sequential yamux read loop used by the default new_host() configuration to block and preventing every stream on that connection from making progress. No fixed version is available as of this review.	2026-08-13	7.5	CVE-2026-73568
Link Factory--Link Factory	The Link Factory WordPress plugin is a backdoor. Distributed as a "homepage sentence publisher", it exposes an operator-controlled REST API under /wp-json/link-factory/v1/ - authenticated by a detached Ed25519 signature verified against a hardcoded operator public key (except for the health check).	2026-08-13	10	CVE-2026-15413
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: geneve: validate inner network offset in geneve_gro_complete() Even with both paths gated on gs->gro_hint, geneve_gro_complete() re-derives the inner dispatch type and length from the packet and the current gs->gro_hint, independently of geneve_gro_receive(). The two can disagree if gs->gro_hint flips under a concurrent geneve_quiesce()/ geneve_unquiesce() (sk_user_data is NULL across a synchronize_net()), or if the re-read option bytes differ from the ones receive parsed. geneve_gro_receive() already records the inner network header position in NAPI_GRO_CB()->inner_network_offset. Have geneve_gro_complete() compute the offset it is about to dispatch at, adding ETH_HLEN in the ETH_P_TEB case where eth_gro_complete() steps over the inner MAC header, and bail out if it lands past inner_network_offset. Use a lower bound rather than exact equality: between gh_len and the inner L3 header, geneve_gro_receive() may also have pulled an inner VLAN tag (vlan_gro_receive() advances the recorded offset past it), which only moves inner_network_offset further out. A valid frame therefore always satisfies inner_nh <= inner_network_offset, while a gh_len inflated by a hint gro_receive() did not honour dispatches past the validated inner header, i.e. the out-of-bounds completion. Only the latter is rejected.	2026-08-15	10	CVE-2026-72407
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: geneve: gate GRO hint in geneve_gro_complete() on gs->gro_hint geneve_gro_receive() reads the GRO hint through geneve_sk_gro_hint_off(), which honours it only when the socket enabled IFLA_GENEVE_GRO_HINT (gs->gro_hint). geneve_gro_complete() instead calls the low-level geneve_opt_gro_hint_off() and acts on the hint unconditionally. On a tunnel without the hint, receive aggregates the frames as plain ETH_P_TEB while complete still honours an attacker-supplied hint option: it inflates gh_len by gro_hint->nested_hdr_len (u8) and redirects the dispatch type, so the inner gro_complete handler runs at nhoff + gh_len, an offset receive never pulled nor validated, reading out of bounds of the skb head: BUG: KASAN: slab-out-of-bounds in ipv6_gro_complete (net/ipv6/ip6_offload.c:196) Read of size 1 at addr ffff88800fe91980 by task exploit/153 ipv6_gro_complete (net/ipv6/ip6_offload.c:196) geneve_gro_complete (drivers/net/geneve.c:965) udp_gro_complete (net/ipv4/udp_offload.c:940) inet_gro_complete (net/ipv4/af_inet.c:1621) __gro_flush (net/core/gro.c:306) Gate the complete path	2026-08-15	10	CVE-2026-72408

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	on gs->gro_hint too via geneve_sk_gro_hint_off(), so both paths agree. Tunnels that enable the hint are unaffected.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv4: fib: Don't ignore error route in local/main tables. When CONFIG_IP_MULTIPLE_TABLES is enabled but no rule is added, fib_lookup() performs route lookup directly on two tables. Since the first lookup does not properly bail out, the result of an error route in the merged local/main table could be overwritten by another route in the default table: # unshare -n # ip link set lo up # ip route add 192.168.0.0/24 dev lo table 253 # ip route add unreachable 192.168.0.0/24 # ip route get 192.168.0.1 192.168.0.1 dev lo table default uid 0 cache <local> Once a random rule is added, the error route is respected: # ip rule add table 0 # ip rule del table 0 # ip route get 192.168.0.1 RTNETLINK answers: No route to host Let's fix the inconsistent behaviour.	2026-08-15	10	CVE-2026-72421
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: cavium/cpt - fix DMA cleanup using wrong loop index The sg_cleanup error path used list[i] instead of list[j] when unmapping DMA buffers, leaking successfully mapped entries and repeatedly unmapping the failed one.	2026-08-15	10	CVE-2026-74279
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: marvell/octeontx - fix DMA cleanup using wrong loop index The sg_cleanup path used list[i] instead of list[j] when unmapping DMA buffers, leaking successfully mapped entries and repeatedly unmapping the failed one.	2026-08-15	10	CVE-2026-74280
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vdpa/octeon_ep: fix IRQ-to-ring mapping in interrupt handler Look up the IRQ index in oct_hw->irqs instead of assuming irq - irqs[0]. This supports non-contiguous IRQ numbers and avoids incorrect ring indexing when irqs[0] is not the base.	2026-08-15	10	CVE-2026-74309
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: use neigh_ha_snapshot() in route_shortcircuit() The neighbour hardware address n->ha can be updated asynchronously by the neighbour subsystem, protected by n->ha_lock seqlock. Reading n->ha without holding the seqlock loop can lead to torn reads or reading a partially updated MAC address. Use neigh_ha_snapshot() in route_shortcircuit() to safely copy n->ha under read_seqbegin()/read_seqretry() lock protection before using it. Note that arp_reduce() and neigh_reduce() seem to have the same issue left for future patches.	2026-08-15	10	CVE-2026-74475
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix path resolution in ksmbd_vfs_kern_path_create The SMB2 open lookup is rooted at the share with LOOKUP_BENEATH, but the create/mkdir/hardlink sink is not: ksmbd_vfs_kern_path_create() builds an absolute path with convert_to_unix_name() and resolves it from AT_FDCWD via start_creating_path(), so a "." component is walked from the real filesystem root and escapes the export. An authenticated client races a missing path component so the rooted open lookup returns -ENOENT (taking the create branch) while the same component is present (a directory) when the create walk runs; the create then resolves "." out of the share. Root the create walk at the share like the lookup and rename paths already are: resolve the parent with vfs_path_parent_lookup(..., LOOKUP_BENEATH, &share_conf->vfs_path) and create the final component with start_creating_noperm(). convert_to_unix_name() then has no callers and is removed.	2026-08-10	9.1	CVE-2026-68083
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: clear sock->sk on the failed-insert path in tipc_sk_create() When tipc_sk_create() fails to insert the new socket (tipc_sk_insert() returns non-zero), its error path frees the sk with sk_free() but leaves sock->sk pointing at the freed object: if (tipc_sk_insert(tsk)) { sk_free(sk); pr_warn("Socket create failed; port number exhausted\n"); return -EINVAL; } This is harmless for plain socket(): the syscall layer clears sock->ops before releasing, so tipc_release() is never called. It is not harmless on the accept() path. tipc_accept() creates the pre-allocated child socket with tipc_sk_create(net, new_sock, 0, kern); on failure it leaves new_sock->sk dangling and new_sock->ops non-NULL, and do_accept() then fput()s the new file, so __sock_release() -> tipc_release() runs lock_sock(new_sock->sk) on the freed sk -- a use-after-free write of the sk_lock spinlock. tipc_release() already guards this exact "failed accept() releases a pre-allocated child" case with "if (sk == NULL) return 0;", but the guard is bypassed because tipc_sk_create() left sock->sk non-NULL (dangling) rather than NULL. Clear sock->sk on the failed-insert path so the existing tipc_release() NULL check fires and the use-after-free is avoided. The tipc_sk_insert() failure is reached when the per-netns socket rhashtable hits its	2026-08-10	9.8	CVE-2026-68117

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	max_size (tsk_rht_params.max_size = 1048576, ~2M elements) -- i.e. once a netns holds ~2M TIPC sockets every insert returns -E2BIG. BUG: KASAN: slab-use-after-free in lock_sock_nested (net/core/socket.c:3839) Write of size 8 at addr ffff8880047cdc38 by task init/1 lock_sock_nested (net/core/socket.c:3839) tipc_release (net/tipc/socket.c:638) __sock_release (net/socket.c:710) sock_close (net/socket.c:1501) __fput (fs/file_table.c:512) Allocated by task 1: sk_alloc (net/core/socket.c:2308) tipc_sk_create (net/tipc/socket.c:487) tipc_accept (net/tipc/socket.c:2744) do_accept (net/socket.c:2034) Freed by task 1: __sk_destruct (net/core/socket.c:2391) tipc_sk_create (net/tipc/socket.c:504) tipc_accept (net/tipc/socket.c:2744) do_accept (net/socket.c:2034)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: openvswitch: fix GSO userspace truncation underflow OVS_ACTION_ATTR_TRUNC currently stores a delta from the original skb length in OVS_CB(skb)->cutlen. When a later userspace action segments a GSO skb, queue_gso_packets() reuses that delta for each smaller segment. A segment can then reach queue_userspace_packet() with cutlen greater than skb->len, underflowing the length passed to skb_zerocopy(). Store the maximum preserved length instead and bound each consumer against the current skb length. Use U32_MAX as the no-truncation sentinel so the value remains valid if skb geometry changes before a consumer handles it.	2026-08-10	9.8	CVE-2026-68123
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mctp: serial: handle zero-length frames to prevent rx buffer overflow The MCTP serial receive state machine reads a frame length byte in mctp_serial_push_header() case 2 and validates it upper-bound-only: if (c > MCTP_SERIAL_FRAME_MTU) { dev->rxstate = STATE_ERR; } else { dev->rxlen = c; dev->rxpos = 0; dev->rxstate = STATE_DATA; ... } A length of zero passes this check, so rxlen is set to 0 and the state machine advances to STATE_DATA. In mctp_serial_push() STATE_DATA, the incoming byte is stored and rxpos incremented before the terminator is dev->rxbuf[dev->rxpos] = c; dev->rxpos++; dev->rxstate = STATE_DATA; if (dev->rxpos == dev->rxlen) { dev->rxpos = 0; dev->rxstate = STATE_TRAILER; } With rxlen == 0 the "rxpos == rxlen" terminator can never fire (rxpos is already 1 on the first data byte), so subsequent bytes are written past the end of the fixed 74-byte rxbuf, which is the last member of the netdev private area. Every following data byte is an attacker-controlled 1-byte out-of-bounds heap write, and the overflow continues until a frame (0x7e) or escape byte resets the parser -- effectively unbounded. Reaching this requires CAP_NET_ADMIN to attach the N_MCTP line discipline and bring the resulting mctpserialN netdev up, after which the bytes arrive via the tty receive path. Route a zero-length frame straight to STATE_TRAILER instead of STATE_DATA. The trailer/framing bytes are still consumed, and the frame resolves to a zero-length skb that the MCTP core rejects; the parser never enters STATE_DATA with rxlen == 0, so the out-of-bounds write can no longer occur. KASAN, on a frame of 0x7e 0x01 0x00 followed by data bytes (before this change): UBSAN: array-index-out-of-bounds in drivers/net/mctp/mctp-serial.c:370 index 74 is out of range for type 'u8 [74]' BUG: KASAN: slab-out-of-bounds in mctp_serial_tty_receive_buf Write of size 1 at addr ... by task kworker/u16:0 mctp_serial_tty_receive_buf tty_ldisc_receive_buf flush_to_ldisc Allocated by task 152: alloc_netdev_mqs mctp_serial_open v2: route zero-length frames to STATE_TRAILER instead of STATE_ERR so the trailer/framing bytes are still consumed (Jeremy Kerr). Found by 0sec automated security-research tooling (https://0sec.ai).	2026-08-10	9.6	CVE-2026-68124
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ila: reload IPv6 header after pskb_may_pull in checksum adjust ila_csum_adjust_transport() caches ip6h = ipv6_hdr(skb) before calling pskb_may_pull(). On a non-linear skb whose transport header sits in a page fragment, pskb_may_pull() can call __pskb_pull_tail() / pskb_expand_head() and free the old skb head, leaving ip6h dangling; the following get_csum_diff(ip6h, p) then reads freed memory. ila_update_ipv6_locator() uses ip6h (and the iaddr derived from it) again after the csum-adjust call and additionally writes the new locator through that pointer. Impact: a remote IPv6 packet routed through a configured ILA csum-adjust-transport route or receive-side mapping triggers a slab-use-after-free in ila_update_ipv6_locator() (KASAN). The route or mapping requires CAP_NET_ADMIN to configure, but trigger packets are unauthenticated once it exists. Reload ip6h after each pskb_may_pull() in ila_csum_adjust_transport() before the csum-diff read. In ila_update_ipv6_locator() only the ILA_CSUM_ADJUST_TRANSPORT case pulls the skb, so reload ip6h and iaddr in that case alone before the destination-address write; the neutral-map modes never pull and keep their cached pointers.	2026-08-10	9.8	CVE-2026-68127

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: gro: fix double aggregation of flush-marked skbs Commit 0ab03f353d36 ("net-gro: Fix GRO flush when receiving a GSO packet.") added a flush check to skb_gro_receive(), but skb_gro_receive_list() lacks the same validation. As a result, packets marked with NAPI_GRO_CB(skb)->flush may still be re-aggregated. This allows already-GRO'd packets with existing frag_list to be re-aggregated into a new GRO session, corrupting the frag_list chain structure. When skb_segment() attempts to unpack these malformed packets, it encounters invalid state and triggers a kernel panic. Scenario (Tethering/Device forwarding): 1. Driver: Generated aggregated packet P1 via LRO with frag_list 2. Dev A: Receives aggregated fraglist packet and flush flag set 3. Dev A: Re-enters GRO, skb_gro_receive_list() is called 4. Missing flush check allows re-aggregation despite flush flag 5. Frag_list chain becomes corrupted (loops or dangling refs) 6. Dev B: TX path calls skb_segment(), crashes on corrupted frag_list Root cause in skb_segment(): The check at line ~4891: if (hsize <= 0 && i >= nfrags && skb_headlen(list_skb) && (skb_headlen(list_skb) == len sg)) { When frag_list is corrupted by double aggregation, when list_skb is a NULL pointer from skb->next, skb_headlen(list_skb) dereference NULL/corrupted pointers occurs. Call Trace: skb_headlen(NULL skb) skb_segment tcp_gso_segment tcp4_gso_segment inet_gso_segment skb_mac_gso_segment __skb_gso_segment skb_gso_segment validate_xmit_skb validate_xmit_skb_list sch_direct_xmit qdisc_restart __qdisc_run qdisc_run net_tx_action Fix: Add NAPI_GRO_CB(skb)->flush validation to the early-return check in skb_gro_receive_list(), matching the defensive programming pattern of skb_gro_receive().	2026-08-10	9.8	CVE-2026-68136
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/x25: fix use-after-free in x25_kill_by_neigh() x25_kill_by_neigh() walks the global X.25 socket list looking for sockets attached to a terminating neighbour. x25_list_lock protects list membership while the lookup is in progress, but it does not pin a socket's lifetime after the lock is dropped. The function currently drops x25_list_lock before calling lock_sock(s). A concurrent close can run x25_release(), remove the same socket from x25_list, and drop the last socket reference in that window. The neighbour teardown path can then lock or inspect a freed struct sock/struct x25_sock. Take sock_hold(s) while x25_list_lock still proves that the list entry is live, then drop the temporary reference after the socket has been locked, rechecked, and released. Recheck x25_sk(s)->neighbour after lock_sock(), because another path may have disconnected the socket before this path acquired the socket lock. Restart the list walk after each disconnect because the list lock was dropped and the previous iterator state may no longer be valid. A QEMU/KASAN run against origin/master reproduced a slab-use-after-free in x25_kill_by_neigh().	2026-08-10	9.8	CVE-2026-68137
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: phonet: pep: fix use-after-free in pep_get_sb() pep_get_sb() doesn't consider that pskb_may_pull() might have relocated the skb data, and continue to access the older pointer, causing UAF. Reproduced under KASAN: BUG: KASAN: slab-use-after-free in pep_get_sb+0x234/0x3b0 Read of size 1 at addr ff11000105510f50 by task repro/157 pep_get_sb+0x234/0x3b0 pipe_handler_do_rcv+0x5f7/0xa10 pep_do_rcv+0x203/0x410 __sk_receive_skb+0x471/0x4a0 phonet_rcv+0x5b3/0x6c0 __netif_receive_skb+0xcc/0x1d0 Refetch the header with skb_header_pointer() after pskb_may_pull(), so the possibly stale pointer is no longer dereferenced. There are better ways to solve this, but, this is the less intrusive one.	2026-08-10	9.8	CVE-2026-68144
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: reject zero bucket types in crush_decode CRUSH bucket type 0 is reserved for devices. The mapper relies on that invariant and uses type 0 to identify leaf devices. If crush_decode() accepts a bucket with type 0, a malformed CRUSH map can make the mapper treat a negative bucket ID as a device and pass it to is_out(), which then indexes the OSD weight array with a negative value. Reject zero bucket types while decoding the CRUSH map so the invalid state never reaches the mapper.	2026-08-10	9.8	CVE-2026-68154
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: refresh auth->authorizer_buf{,_len} after authorizer update ceph_x_create_authorizer() caches au->buf->vec.iov_base and au->buf->vec.iov_len in struct ceph_auth_handshake. These cached values are then used by the messenger connect code when sending the authorizer. ceph_x_update_authorizer() can rebuild the authorizer when a newer service ticket is available. If the rebuilt authorizer no longer fits in the existing buffer, ceph_x_build_authorizer() drops its reference to au->buf and allocates a new one. If this is the final reference, ceph_buffer_put() frees the old ceph_buffer and its vec.iov_base, but auth-	2026-08-10	9.8	CVE-2026-68156

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	>authorizer_buf still points at that freed memory. A subsequent msgr1 reconnect can therefore queue the stale pointer and trigger a KASAN slab-use-after-free in _copy_from_iter() while tcp_sendmsg() copies the authorizer. Refresh auth->authorizer_buf and auth->authorizer_buf_len after a successful authorizer rebuild so the messenger sends the current buffer.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: Fix multiplication overflow in decode_new_up_state_weight() If a message of type CEPH_MSG_OSD_MAP contains a (maliciously) corrupted osdmap, out-of-bounds memory accesses may occur in decode_new_up_state_weight(). This happens because the bounds check for the new_state part is based on calculating its length depending on a len value read from the incoming message. This calculation may overflow leading to an incorrect bounds check. Subsequently, out-of-bounds reads may occur when decoding this part. This patch switches the multiplication to use check_mul_overflow() to abort processing the osdmap if an overflow occurred. Therefore, osdmaps/messages containing large values for len that result in a multiplication overflow are treated as invalid. [idryomov: rename new_state_len -> new_state_item_size, formatting]	2026-08-10	9.8	CVE-2026-68158
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: bound pg_{temp,upmap,upmap_items} length to CEPH_PG_MAX_SIZE __decode_pg_temp() decodes an user-controlled length but only rejects values large enough to overflow the allocation; it does not bound it to CEPH_PG_MAX_SIZE. The helper backs both pg_temp and pg_upmap decoding, and apply_upmap()/get_temp_osds() later copy the decoded list into the fixed-size on-stack array struct ceph_osds.osds[CEPH_PG_MAX_SIZE]. A monitor that sends an OSDMap with a pg_temp/pg_upmap entry longer than 32 thus causes a stack out-of-bounds write. An OSD set for a single PG can never exceed CEPH_PG_MAX_SIZE, so reject longer entries at decode time. The bound is well below the old overflow threshold, so it also covers the allocation-size overflow the previous check guarded against. BUG: KASAN: stack-out-of-bounds in ceph_pg_to_up_acting_osds Write of size 4 ... by task exploit kasan_report (mm/kasan/report.c:595) ceph_pg_to_up_acting_osds (net/ceph/osdmap.c:2617 net/ceph/osdmap.c:2833) calc_target (net/ceph/osd_client.c:1638) __submit_request (net/ceph/osd_client.c:2394) ceph_osdc_start_request (net/ceph/osd_client.c:2490) ceph_osdc_call (net/ceph/osd_client.c:5164) rbd_dev_image_probe (drivers/block/rbd.c:6899) do_rbd_add (drivers/block/rbd.c:7138) ... kernel BUG at net/ceph/osdmap.c:2670! [idryomov: do the same in __decode_pg_upmap_items()]	2026-08-10	9.8	CVE-2026-68159
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ceph: fix pre-auth out-of-bounds read on snaptrace in ceph_handle_caps() ceph_handle_caps() reads snap_trace_len from the wire-format ceph_mds_caps header and uses it unconditionally to build a fake end pointer (snaptrace + snaptrace_len) that is later handed to ceph_update_snap_trace() in the CEPH_CAP_OP_IMPORT case: snaptrace = h + 1; snaptrace_len = le32_to_cpu(h->snap_trace_len); p = snaptrace + snaptrace_len; ... case CEPH_CAP_OP_IMPORT: if (snaptrace_len) { ... if (ceph_update_snap_trace(mdsc, snaptrace, snaptrace + snaptrace_len, false, &realm)) { ... } ceph_update_snap_trace() then decodes a struct ceph_mds_snap_realms from snaptrace using ceph_decode_need(&p, e, sizeof(*ri), bad) with the attacker-supplied fake end e == snaptrace + snaptrace_len. With snaptrace_len == 0xFFFFFFFF the bound check is trivially satisfied, ri = p reads sizeof(struct ceph_mds_snap_realms) past the legitimate msg->front buffer, and ri->num_snaps / ri->num_prior_parent_snaps then drive further out-of-bounds reads of the encoded snap arrays. The eleven msg_version >= 2 .. msg_version >= 12 decoder blocks above the op switch each catch this OOB through their ceph_decode_*_safe() / ceph_decode_need() helpers, but they sit behind a hdr.version-gated if, so a malicious or compromised MDS that sets msg->hdr.version = 1 reaches the IMPORT path with no version-gated decoder having validated snap_trace_len. The shape has been present since ceph_handle_caps() was introduced. Validate snap_trace_len against the message front buffer before consuming it, using the canonical ceph_decode_need() / ceph_has_room() helper. The helper bounds the length with subtraction (n <= end - p, guarded by end >= p) rather than pointer addition, so it is wrap-safe for the attacker-controlled u32 length on 32-bit builds where p + snap_trace_len could overflow the address space. This matches the rest of the ceph decode path (e.g. the pool_ns_len check a few lines below), and the existing goto bad cleanup already covers this exit path.	2026-08-10	9.8	CVE-2026-68160

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: close UDP tunnel sockets during netns teardown proc_sctp_do_udp_port() starts per-net SCTP UDP tunneling sockets when net.sctp.udp_port is set, and stops/restarts them when the sysctl value changes. The netns exit path does not stop these sockets, so a namespace can be torn down while its SCTP UDP tunnel sockets are still installed. Close the UDP tunnel sockets from sctp_ctrlsock_exit() after unregistering the per-net sysctl table. This prevents new sysctl writes from racing in while the sockets are being released, and closes the sockets before the control socket is destroyed.	2026-08-10	9.8	CVE-2026-68161
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix stale skb->sk reference on subflow close The backlog list is updated by mptcp_data_ready() under mptcp_data_lock(). The cleanup of backlog references to a closing subflow, however, was performed in mptcp_close_ssk(), before __mptcp_close_ssk() acquires the ssk lock, and while holding neither the ssk lock nor mptcp_data_lock(). Because that traversal ran without mptcp_data_lock(), concurrent softirq RX processing on another CPU (subflow_data_ready() -> mptcp_data_ready() -> __mptcp_add_backlog(), under mptcp_data_lock()) could add a backlog entry referencing the ssk while the cleanup loop was in progress. Such an entry could be missed by the cleanup, or the concurrent list update could corrupt the traversal, leaving skb->sk pointing at the ssk after it is freed. A later mptcp_backlog_purge() then dereferences the stale pointer, triggering a warning in inet_sock_destruct() (skb->sk_rmem_alloc != 0) followed by a use-after-free in mptcp_backlog_purge(). Fix this by moving the backlog cleanup into __mptcp_close_ssk(), after subflow->closing is set to 1 and while the ssk lock is still held, serialized under mptcp_data_lock(). The cleanup runs only on the push path (MPTCP_CF_PUSH), where backlog references accumulate; on other teardown paths the caller already handles cleanup. With subflow->closing set and mptcp_data_lock() held across the purge, any concurrent mptcp_data_ready() either completes its enqueue before the purge runs and is caught, or observes closing=1 and bails out. Once mptcp_data_unlock() is reached, no new skb referencing the ssk can be enqueued, so the cleanup is exhaustive. Remove the unprotected traversal from mptcp_close_ssk() entirely.	2026-08-10	9.8	CVE-2026-68170
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: auth: verify auth requirement when auth_chunk is NULL sctp_auth_chunk_verify() returns true unconditionally when chunk->auth_chunk is NULL, silently skipping authentication. This is incorrect when: 1. skb_clone() failed in the BH receive path, leaving auth_chunk NULL. In sctp_endpoint_bh_rcv() asoc is NULL for new connections, so the early sctp_auth_rcv_cid() check cannot catch this. 2. No AUTH chunk precedes COOKIE-ECHO, so skb_clone() is never called and auth_chunk remains NULL. Fix by checking sctp_auth_rcv_cid() when auth_chunk is NULL: if authentication is required, return false to drop the chunk; otherwise continue normally.	2026-08-10	9.8	CVE-2026-68300
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: amt: re-read skb header pointers after every pull Several AMT receive and transmit paths cache a pointer into the skb head (ip_hdr(), ipv6_hdr(), eth_hdr() or the AMT message header) and then call a helper that can reallocate that head before the cached pointer is used again. pskb_may_pull(), ip_mc_may_pull(), ipv6_mc_may_pull(), iptunnel_pull_header(), ip_mc_check_igmp() and ipv6_mc_check_mld() can all free the old head and move the data, so a pointer taken before the call dangles afterwards and the later access is a use-after-free of the freed head. The affected sites are: amt_rcv() caches ip_hdr() before amt_parse_type() pulls, then reads iph->saddr. amt_dev_xmit() caches ip_hdr()/ipv6_hdr() before ip_mc_check_igmp()/ipv6_mc_check_mld() and pskb_may_pull(), then reads the group address. amt_multicast_data_handler() caches eth_hdr() before pskb_may_pull(), then writes the L2 header. amt_membership_query_handler() caches the AMT header, the outer and inner eth_hdr() and ip_hdr() before iptunnel_pull_header() and several pulls, then reads and writes them. amt_igmpv3_report_handler() and amt_mldv2_report_handler() cache ip_hdr()/ipv6_hdr() and the current group record and read the record count from the report header inside the record loop, across the *_mc_may_pull() calls. amt_update_handler() caches ip_hdr() and the AMT membership-update header before pskb_may_pull(), iptunnel_pull_header(), ip_mc_check_igmp() and the report handler, then reads iph->daddr and amtmu->nonce / amtmu->response_mac. Fix each site by either snapshotting the scalar that is used after the pull before the first pull runs, or re-deriving the header pointer from the skb after the last pull that can move the head. Values that are stable across the pull (source and group address, the response MAC and nonce, the	2026-08-10	9.8	CVE-2026-68302

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	record count, the outer source MAC) are snapshotted; pointers that are written through or read repeatedly are re-derived.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: smb: client: validate DFS referral PathConsumed parse_dfs_referrals() validates that the response contains the fixed referral entry array and, on for-next, the per-referral string offsets. However, the response also contains a PathConsumed value that is later used for DFS path parsing. If a malformed response provides a PathConsumed value larger than the search name, later DFS parsing can advance beyond the end of the path. Validate PathConsumed against the search name length before storing it in the parsed referral.	2026-08-10	9.1	CVE-2026-68343
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: pin conn during async oplock break notification smb2_oplock_break_noti() and smb2_lease_break_noti() store a ksmbd_conn pointer in an async ksmbd_work and then queue that work on ksmbd-io. The work only increments conn->r_count, which prevents teardown from passing the pending-request wait after the increment, but it does not pin the struct ksmbd_conn object. If connection teardown races with an oplock break notification, the last conn reference can be dropped before the queued worker finishes. The worker then uses the freed conn in ksmbd_conn_write() and ksmbd_conn_r_count_dec(). Take a real conn reference when publishing the conn pointer to the async work item, and drop it after the notification work has decremented r_count. Apply the same lifetime rule to lease break notification, which uses the same work->conn pattern.	2026-08-10	9.8	CVE-2026-68381
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/checksum: Fix csum_partial() without vector facility Currently csum_partial() calls csum_copy() with copy=false and dst=NULL. On machines without the vector facility, csum_copy() falls back to cksum(dst, ...), causing the checksum to be calculated from address zero instead of the source buffer. The VX implementation already checksums data loaded from src. Make the fallback do the same by passing src to cksum().	2026-08-10	9.8	CVE-2026-68385
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: smb/client: handle overlapping allocated ranges in fallocate smb3_simple_fallocate_range() can skip holes when an allocated range returned by the server starts before the current fallocate offset. The skipped hole is not zero-filled, but fallocate still returns success. A later write to that hole may therefore fail with ENOSPC. The function queries allocated ranges so that it can preserve existing contents and write zeroes only into holes. However, the server may return a range that starts before the current fallocate offset. For example, assume the fallocate request is [100, 400) and the only allocated range returned by the server is [0, 200): Request: [100, 400) Server range: [0, 200) allocated Correct: [100, 200) allocated data, skip [200, 400) hole, zero-fill Current: [100, 300) skipped [300, 400) zero-filled afterwards The current code adds the full server range length, 200, to the current offset 100 and moves to 300. As a result, the hole in [200, 300) is skipped without being zero-filled. Fix this by advancing only over the part of the allocated range that overlaps the current fallocate offset. Ignore ranges that end before the current offset and reject ranges whose end offset overflows. This also prevents a malformed range length from causing an out-of-bounds zero-buffer read.	2026-08-10	9.8	CVE-2026-68388
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: fix stale skb->prev after async crypto steals a GSO segment skb_gso_segment() leaves the segment list head with ->prev pointing at the last segment, an invariant validate_xmit_skb_list() relies on when it sets its tail pointer (tail = skb->prev). When validate_xmit_xfrm() walks a GSO list and some segments are stolen by async crypto (->xmit() returns -EINPROGRESS), those segments are unlinked from the list but the head ->prev is never updated. If the last segment is the one stolen, the returned head still has ->prev pointing at it, even though it is now owned by the crypto engine and may be freed. validate_xmit_skb_list() later does tail->next = skb, writing through that stale pointer -- a use-after-free. Repoint skb->prev at the last retained segment before returning.	2026-08-10	9.8	CVE-2026-68426
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate minimum PDU size for transform requests The receive path applies the minimum SMB2 PDU size check only when ProtocolId is SMB2_PROTO_NUMBER. A packet carrying SMB2_TRANSFORM_PROTO_NUM bypasses the check even when the negotiated dialect does not provide transform handling. On an SMB 2.1 connection, a short transform packet therefore reaches init_smb2_rsp_hdr(), which interprets the request as a full SMB2 header and reads beyond the request	2026-08-12	9.1	CVE-2026-68431

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allocation. The copied fields can then be returned to the unauthenticated client. Compression transforms are converted to ordinary SMB2 messages before protocol validation. After that conversion, validate ordinary SMB2 requests against SMB2_MIN_SUPPORTED_PDU_SIZE and require encryption transform requests to contain both a transform header and an SMB2 header. This rejects truncated requests before work allocation.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: use opener credentials for FSCTL mutations SET_SPARSE, SET_ZERO_DATA and SET_COMPRESSION operate on an open SMB handle but call VFS xattr, fallocation or fileattr helpers with the current ksmbd worker credentials. Those helpers can revalidate inode permissions, ownership and LSM policy independently of the SMB handle access mask. Run each operation with the credentials captured in the target file when the handle was opened. Keep credential handling local to these single-file FSCTLs rather than applying session credentials to the complete IOCTL handler, which also contains handle-less and multi-handle operations.	2026-08-15	9.1	CVE-2026-68457
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: reload ip header after head reallocation __ip_vs_get_out_rt() calls skb_ensure_writable() which may reallocate skb->head.	2026-08-15	9.8	CVE-2026-68476
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix more places with wrong ipv6 transport offsets Sashiko reports for more incorrect IPv6 transport offsets. The app code for TCP was assuming IPv4 network header even after the ipvsh argument was provided. This can cause problems with apps over IPv6. As for the only official app in the kernel tree (FTP) this problem is harmless because we use Netfilter to mangle the FTP ports and we do not adjust the TCP seq numbers. Also, provide correct offset of the ICMPV6 header in ip_vs_out_icmp_v6() for correct checksum checks when the IPv6 packet has extension headers.	2026-08-15	9.8	CVE-2026-68477
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drbd: reject data replies with an out-of-range payload size recv_dless_read() receives a P_DATA_REPLY from a peer into the bio of an outstanding read request. The peer-supplied payload length reaches it as the signed int data_size, and two peer-controlled inputs can make it negative. With a negotiated data-integrity-alg the digest length is subtracted first, so a reply whose payload is smaller than the digest underflows data_size. With no integrity algorithm (the default) data_size is assigned from the unsigned h95/h100 wire length and drbdd() never bounds it for a payload-carrying command, so a length above INT_MAX casts it negative; this path needs no non-default feature. The bio receive loop then computes expect = min_t(int, data_size, bv_len), which is negative, and drbd_recv_all_warn(mapped, expect) receives with a size_t of SIZE_MAX into the first mapped page. The sibling receive path read_in_block() is not affected: it uses an unsigned size and rejects it against DRBD_MAX_BIO_SIZE before receiving. Reject a data reply whose size is negative after the optional digest subtraction, covering both triggers. Impact: a malicious or man-in-the-middle DRBD peer copies attacker-chosen bytes past a bio page in the receiver, corrupting kernel memory. A node that reads from its peer (a diskless node, or read-balancing to the peer) is exposed in the default configuration; data-integrity-alg is not required.	2026-08-15	9.8	CVE-2026-72014
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: reset full ip_vs_seq structs in ip_vs_conn_new Commit 9a05475cebdd ("ipv6: avoid kmem_cache_zalloc in ip_vs_conn_new") changed ip_vs_conn_new() to allocate an ip_vs_conn object with kmem_cache_alloc(). The function then initializes many fields explicitly, but only resets in_seq.delta and out_seq.delta in the two struct ip_vs_seq members. That leaves init_seq and previous_delta uninitialized. This is normally harmless while the corresponding IP_VS_CONN_F_IN_SEQ or IP_VS_CONN_F_OUT_SEQ flag is clear. For connections learned from a sync message, however, ip_vs_proc_conn() preserves those flags from IP_VS_CONN_F_BACKUP_MASK and passes opt=NULL when the message omits IPVS_OPT_SEQ_DATA. In that case the new connection can be hashed with SEQ flags set but with the rest of in_seq/out_seq still containing stale slab data. When a packet for such a connection is later handled by an IPVS application helper, vs_fix_seq() and vs_fix_ack_seq() use previous_delta and init_seq to rewrite TCP sequence numbers. A malformed sync message can therefore make forwarded packets carry stale slab bytes in their TCP seq/ack numbers, and can also corrupt the forwarded TCP flow. Reset both struct ip_vs_seq members completely before publishing the connection. This matches the existing "reset struct ip_vs_seq"	2026-08-15	9.8	CVE-2026-72020

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	comment and keeps the sequence-adjustment gates inactive unless valid sequence data is installed later.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: orangefs: keep the readdir entry size 64-bit in fill_from_part() fill_from_part() computes the size of a directory entry in size_t but stores it in a __u32. An entry length near U32_MAX wraps it to a small value, bypasses the bounds check, and is then used to index the entry, reading far past the directory part -- an out-of-bounds read that oopses the kernel. Compute the size as a u64 so it cannot truncate; the bounds check then rejects the entry. The trailer is supplied by the userspace client.	2026-08-15	9.8	CVE-2026-72033
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: espintcp: use sk_msg_free_partial to fix partial send sk_msg_free_partial() ensures consistency of the skmsg at every iteration, without having to manually handle uncharges and offsets. This simplifies the code, and fixes some bugs in skmsg accounting when we don't send the full contents.	2026-08-15	9.8	CVE-2026-72041
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gve: fix header buffer corruption with header-split and HW-GRO The DQO RX datapath programs a per-buffer-queue-descriptor header_buf_addr at post time and reads the split header back at completion time. Both the post and the read currently index the header buffer by queue position rather than by the buffer's identity: - post (gve_rx_post_buffers_dqo): header_buf_addr is computed from bufq->tail - read (gve_rx_dqo): the header is read from desc_idx (the completion queue head index) This relies on the buffer-queue index and the completion-queue index being equal for the start of every packet, i.e. on the device consuming posted buffers and returning completions in the exact same order. That assumption does not hold once HW-GRO is enabled with multiple flows: coalesced segments are accepted and completed in an order that may differ from the order buffers were posted, and segments from different flows may interleave. That results in two problems: 1. Wrong header slot on read. Because the read offset is derived from the completion index (desc_idx) while the device wrote the header to the address programmed for the buffer's buf_id, the driver can copy a header belonging to a different packet. This shows up as throughput drop (about 30% drop and large numbers of TCP retransmissions) with header-split and HW-GRO both enabled and many streams. 2. Header buffer reused while still owned by the device. The driver advances bufq->head by one per completion and re-posts buffers based on that. Arrival of N RX completions only guarantees that at least N RX buffer descriptors have been read by the device. It does not guarantee that the device has relinquished the ownership of all the buffers corresponding to those N descriptors. With out-of-order completions (e.g. the completion for a packet copied into buffer N arrives before the completion for a packet copied into buffer N-1), the driver can re-post and overwrite a header buffer that the device is still going to write into, corrupting the header of a packet whose completion has not yet been processed. Fix both issues by indexing the header buffer by buf_id on both the post and read paths. Reading from buf_id's slot is therefore always correct regardless of completion ordering (fixes problem 1). Indexing by buf_id also ties each header slot to the lifetime of its buffer state. A buffer state is only returned to the free/recycle lists when its own completion (buf_id) is processed, so its header slot can only be re-posted after the device is done with it. This makes header slot reuse safe under out-of-order completions (fixes problem 2). Allocate (gve_rx_alloc_hdr_bufs) and free (gve_rx_free_hdr_bufs) the header buffers based on num_buf_states to match the buf_id indexing.	2026-08-15	9.8	CVE-2026-72046
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mana: Sync page pool RX frags for CPU MANA allocates RX buffers from page pool fragments when frag_count is greater than 1. In that case the buffers remain DMA mapped by page pool and the RX completion path does not call dma_unmap_single(). As a result, the implicit sync-for-CPU normally performed by dma_unmap_single() is missing before the packet data is passed to the networking stack. This breaks RX on configurations which require explicit DMA syncing, for example when booted with swiotlb=force. Fix this by recording the page pool page and DMA sync offset when the RX buffer is allocated, and syncing the received packet range for CPU access before handing the RX buffer to the stack.	2026-08-15	9.8	CVE-2026-72064
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mana: Validate the packet length reported by the NIC Validate the packet length reported in the RX CQE before passing it to skb processing. The CQE is supplied by the NIC device and should not be blindly trusted.	2026-08-15	9.8	CVE-2026-72065

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: locking/rt: Fix the incorrect RCU protection in rt_spin_unlock() rt_spin_unlock() releases the RCU protection before unlocking the lock. That opens the door for the following UAF scenario: T1 T2 spin_lock(&p->lock); rcu_read_lock(); invalidate(p); p = rcu_dereference(ptr); rcu_assign_pointer(ptr, NULL); if (!p) return; spin_unlock(&p->lock); spin_lock(&p->lock) lock(&lock->lock); rcu_read_lock(); kfree_rcu(p); rcu_read_unlock(); spin_unlock(&p->lock) rcu_read_unlock(); // Ends grace period rcu_do_batch() kfree(p); UAF -> rt_mutex_cmpxchg_release(&lock->lock...) Regular spinlocks keep preemption disabled across the unlock operation, which provides full RCU protection, but the RT substitution fails to resemble that. Same applies for the rwlock substitution. Move the rcu_read_unlock() invocation past the unlock operations to match the non-RT semantics. This makes it asymmetric vs. rt_xxx_lock(), but that's harmless as the caller needs to hold RCU read lock across the lock operation. The migrate_enable() call stays before the unlock operation because there is no per CPU operation in the unlock path which would require migration to be kept disabled.	2026-08-15	9.8	CVE-2026-72069
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: target: core: Fix iSCSI ISID use-after-free in REGISTER AND MOVE core_scsi3_emulate_pro_register_and_move() maps the PERSISTENT RESERVE OUT parameter list with transport_kmap_data_sg() and parses the destination TransportID with target_parse_pr_out_transport_id(). For an iSCSI TransportID (FORMAT CODE 01b), iscsi_parse_pr_out_transport_id() returns the ISID in iport_ptr as a raw pointer into that mapped buffer. The function then unmaps the buffer with transport_kunmap_data_sg() before dereferencing iport_ptr in strcmp(), __core_scsi3_locate_pr_reg() and core_scsi3_alloc_registration(). When the parameter list spans more than one page (PARAMETER LIST LENGTH > 4096), transport_kmap_data_sg() uses vmap() and transport_kunmap_data_sg() does vunmap(), so the kernel virtual address backing iport_ptr is torn down and every subsequent dereference is a use-after-free read of the unmapped region. Keep the parameter list mapped until iport_ptr is no longer needed: drop the early transport_kunmap_data_sg() and unmap once on the success path, right before returning. The error paths already unmap through the existing "if (buf) transport_kunmap_data_sg(cmd)" at the out: label, which now runs on every post-map error exit because buf is no longer cleared early. Only reads of the mapping happen while spinlocks are held; the map and unmap calls remain outside any lock. The sibling caller core_scsi3_decode_spec_i_port() already uses the buffer before unmapping it and is left unchanged.	2026-08-15	9.8	CVE-2026-72083
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: target: Bound PR-OUT TransportID parsing to the received buffer core_scsi3_decode_spec_i_port() and core_scsi3_emulate_register_and_move() hand the raw PERSISTENT RESERVE OUT parameter buffer to target_parse_pr_out_transport_id() without telling it how many bytes are valid. For an iSCSI TransportID (FORMAT CODE 01b), iscsi_parse_pr_out_transport_id() locates the ",i,0x" ISID separator with an unbounded strstr() (and on the error path prints the name with a further unbounded "%s"). An initiator can submit a TransportID whose iSCSI name contains neither a ",i,0x" substring nor a NUL terminator, filling the parameter list to its end, so the scan runs off the end of the buffer. When the parameter list spans more than one page the buffer is a multi-page vmap (transport_kmap_data_sg()), so the over-read walks into the trailing vmalloc guard page and oopses (KASAN: vmalloc-out-of-bounds in strstr). It is reachable by any fabric that delivers a PR OUT to a device exported through an iSCSI TPG, including a guest via vhost-scsi. Pass the number of received bytes down to the parser and validate the iSCSI TransportID's own self-described length (ADDITIONAL LENGTH + 4) once, up front: reject it if it is below the spc4r17 minimum or larger than the received buffer, then bound the separator search, the ISID walk and the name copy by that length. This is the length check the callers already perform after the parse (core_scsi3_decode_spec_i_port() compares tid_len against tpdid, core_scsi3_emulate_register_and_move() validates it against data_length), moved ahead of the scan. Also drop the unbounded "%s" of the unterminated name. Add per-format explicit name-length checks before copying into i_str, rather than silently truncating with min_t: for FORMAT CODE 00b reject if the descriptor body (tid_len - 4 bytes) cannot fit in i_str[TRANSPORT_IQN_LEN]; for FORMAT CODE 01b reject if the name portion (from &buf[4] up to the separator) cannot fit. Both checks make the bounds intent explicit at each format	2026-08-15	9.8	CVE-2026-72084

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	branch. While here, also reject a FORMAT CODE 01b TransportID whose ",i,0x" separator sits at the very end of the descriptor: that leaves an empty ISID and points the returned port nexus pointer at buf + tid_len, one past the descriptor, which the registration code (__core_scsi3_locate_pr_reg(), __core_scsi3_alloc_registration()) then dereferences as the ISID string -- the same over-read of the parameter buffer for a malformed descriptor.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: xen: scsiback: Free unsubmitted command instead of double-putting it scsiback_get_pend_req() obtains a command tag and returns a vscsibk_pend whose embedded se_cmd has only been memset to 0, so its cmd_kref is 0; the se_cmd is initialised (kref_init()) via target_init_cmd() only later, in scsiback_cmd_exec(), on the successful VSCSIIF_ACT_SCSI_CDB path. The two error paths in scsiback_do_cmd_fn() taken before the command is submitted -- a failed scsiback_gnttab_data_map() and an unknown ring_req.act -- call transport_generic_free_cmd(&pending_req->se_cmd, 0), which kref_put()s a refcount of 0. That underflows it ("refcount_t: underflow; use-after-free") and, as the release function is not run, leaks the command tag. Impact: a pvSCSI guest can leak every command tag of a LUN's session, stopping the LUN, by submitting requests with a bad grant reference or an unknown request type; under panic_on_warn the refcount underflow panics the host. Add a helper that just returns the tag with target_free_tag() and sends the error response. It frees the tag while the v2p reference still pins the session, and snapshots the response fields beforehand because freeing the tag can let another ring reuse the pending_req slot.	2026-08-15	9.3	CVE-2026-72085
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm-verity: fix buffer overflow in FEC calculation There's a buffer overflow in dm-verity-fec: if (neras && *neras <= v->fec->roots) fio->erasures[(*neras)++] = i; This allows *neras to reach roots + 1 (the post-increment pushes it past roots). This value is then passed as no_eras to decode_rs8(). Inside the RS decoder (lib/reed_solomon/decode_rs.c:113-121), the erasure locator polynomial loop writes lambda[j] where j can reach nroots + 1 - one element past the end of lambda[] (which is sized nroots + 1, valid indices 0..nroots). The out-of-bounds write lands on syn[0], corrupting the syndrome buffer.	2026-08-15	9.8	CVE-2026-72098
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvmet-rdma: handle inline data with a nonzero offset nvmet_rdma_use_inline_sg() maps the host-controlled inline data offset into the per-command inline scatterlist. The bounds check admits any offset with off + len <= inline_data_size, but the mapping still assumes the data begins in the first inline page: sg->offset = off; sg->length = min_t(int, len, PAGE_SIZE - off); When a port is configured with inline_data_size > PAGE_SIZE (settable up to max(SZ_16K, PAGE_SIZE)), an offset in (PAGE_SIZE, inline_data_size] makes "PAGE_SIZE - off" underflow, so sg->length is set to ~4 GiB and the block backend reads far past the first inline page. num_pages(len) also ignores the offset, so an in-bounds offset whose [off, off+len) span crosses a page boundary under-counts the scatterlist. Map the offset properly: split it into a page index and an in-page offset, start the scatterlist at that page, and size the page count from page_off + len. Because the request scatterlist may now start at inline_sg[page_idx] rather than inline_sg[0], generalize the inline-SGL identity test in nvmet_rdma_release_rsp() to a range test; otherwise the persistent inline scatterlist is mistaken for an allocated one and nvmet_req_free_sgls() frees an inline page (and warns in free_large_kmalloc()).	2026-08-15	9.8	CVE-2026-72129
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvmet-auth: reject short AUTH_RECEIVE buffers nvmet_execute_auth_receive() trusts the AUTH_RECEIVE allocation length after checking only that it is nonzero and matches the transfer length. In the SUCCESS1 and FAILURE1/default states, that lets a remote NVMe-oF initiator reach the fixed-size DH-HMAC-CHAP response builders with a kmalloc() buffer shorter than the response, so nvmet_auth_success1() and nvmet_auth_failure1() write past the allocation; both only WARN_ON the short length and then format the message anyway. Impact: A remote NVMe-oF initiator with access to an auth-enabled target can trigger a 16-byte heap out-of-bounds write via a one-byte AUTH_RECEIVE allocation length. Compute the minimum response length for the current DH-HMAC-CHAP step in nvmet_auth_receive_data_len() and report a zero data length when the host-supplied allocation length is shorter, so the existing zero-length check in nvmet_execute_auth_receive() rejects the command before any builder runs. The SUCCESS1 minimum is sizeof(struct nvme_auth_dhchap_success1_data) plus the	2026-08-15	9.8	CVE-2026-72130

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HMAC hash length, because the response hash is written into the rval[] flexible-array tail, so the minimum is state dependent rather than a flat sizeof. CHALLENGE keeps its existing variable-length guard in nvmet_auth_challenge(). This is reachable only when in-band DH-HMAC-CHAP authentication is configured on the target.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: nat_keepalive: avoid double free on send error nat_keepalive_send() frees the keepalive skb whenever the IPv4 or IPv6 send helper reports an error. That cleanup is only correct before the skb is handed to the output path. Once ip_build_and_send_pkt() or ip6_xmit() takes ownership, the networking stack may already have consumed the skb before returning an error, so freeing it again is unsafe. Handle the pre-handoff failure cases inside nat_keepalive_send_ipv4() and nat_keepalive_send_ipv6(), where the caller still owns the skb, and keep nat_keepalive_send() responsible only for family dispatch and the unsupported-family cleanup path.	2026-08-15	9.8	CVE-2026-72137
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: defer md5sig_info kfree past RCU grace period in tcp_connect The md5+ao reconciliation in tcp_connect() (net/ipv4/tcp_output.c) has two symmetric branches: if (needs_md5) { tcp_ao_destroy_sock(sk, false); } else if (needs_ao) { tcp_clear_md5_list(sk); kfree(rcu_replace_pointer(tp->md5sig_info, NULL, ...)); } Both branches free a per-socket auth-info object while the socket is in TCP_SYN_SENT and is already on the inet ehash (inserted by inet_hash_connect() in tcp_v4_connect()). Both branches are reachable by softirq RX-path readers that load the corresponding info pointer via implicit RCU before bh_lock_sock_nested() is taken. The needs_md5 branch is fixed in the prior patch by re-introducing the call_rcu() free in tcp_ao_destroy_sock(): the equivalent per-key loop runs inside tcp_ao_info_free_rcu(), the RCU callback, so by the time it frees each tcp_ao_key all softirq readers that captured the container have already completed rcu_read_unlock(). The needs_ao branch is not symmetric in the same way. The container free can be deferred via kfree_rcu(md5sig, rcu) -- struct tcp_md5sig_info already has the required rcu member (include/net/tcp.h:1999-2002), and the rest of the tree already does this in the tcp_md5sig_info_add() rollback paths (net/ipv4/tcp_ipv4.c:1410, 1436). But the per-key teardown is done by tcp_clear_md5_list() in process context BEFORE the container's RCU grace period: it walks &md5sig->head and frees each tcp_md5sig_key with bare hlist_del + kfree. A concurrent softirq reader in __tcp_md5_do_lookup() / __tcp_md5_do_lookup_exact() (tcp_ipv4.c:1253, 1298) walks the same list via hlist_for_each_entry_rcu() and races with that bare kfree on the keys themselves -- a per-key slab use-after-free of the same class as the TCP-AO bug, on the same race window. Fix this in two halves: 1. Convert the bare kfree() in tcp_connect() to kfree_rcu() so the md5sig_info container joins the rest of the md5sig lifecycle. The local-variable lift is mechanical and required because kfree_rcu() is a macro that expects an lvalue. 2. Make tcp_clear_md5_list() RCU-safe by replacing hlist_del + kfree(key) with hlist_del_rcu + kfree_rcu(key, rcu). struct tcp_md5sig_key already carries the rcu member (include/net/tcp.h:1995) and tcp_md5_do_del() (net/ipv4/tcp_ipv4.c:1456) already uses kfree_rcu, so this restores the lifecycle invariant the rest of the file follows rather than introducing a one-off. The other caller of tcp_clear_md5_list() is tcp_md5_destruct_sock() (net/ipv4/tcp.c:412), which runs from the sock destructor when the socket is already unhashed and unreachable; the extra grace period there is unnecessary but harmless. Making the helper unconditionally RCU-safe is the cleaner contract. The needs_ao branch is not reachable by the users reproducer used to demonstrate the AO-side splat (the repro installs both keys but ends up in the needs_md5 branch because the connect peer matches the MD5 key, not the AO key); however the symmetric race exists and a maintainer touching this code should not have to think about which branch escapes RCU and which one does not. [also credits to Qihang, who found that this races with tcp-diag]	2026-08-15	9.8	CVE-2026-72139
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: fix WARN_ON for resident attribute in ntfs_map_runlist_nolock() When ntfs_map_runlist_nolock() needs to look up the attribute extent containing a target VCN (ctx_needs_reset == true), it calls ntfs_attr_lookup() and then expects the result to be a non-resident attribute, since only non-resident attributes have a mapping pairs array to decompress. A crafted NTFS image can place a resident attribute where a non-resident one is expected, causing ntfs_attr_lookup() to succeed but return a resident attribute record. Previously this was caught only by a	2026-08-15	9.8	CVE-2026-72185

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WARN_ON(), which does not stop execution. The code then falls through to read a->data.non_resident.highest_vcn from what is actually a resident attribute, accessing the wrong union member and corrupting the VCN range check. The caller path triggering this warning during mount is: ntfs_map_runlist_nolock ntfs_empty_logfile load_system_files ntfs_fill_super In this path ctx is NULL, so ntfs_map_runlist_nolock() allocates a temporary search context internally and sets ctx_needs_reset = true. The existing resident-attribute guard in the ctx != NULL branch already returns -EIO silently for the same condition; make the ctx_needs_reset path consistent by replacing the WARN_ON() with the same -EIO error return. This causes the crafted image to be rejected with a mount error instead of triggering a kernel warning.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: make system files immutable to prevent corruption When a system file such as \$Bitmap is exposed via show_sys_files and written from userspace, the volume is corrupted and, because the cluster allocator scans \$Bitmap through the same inode's page cache, a write to \$Bitmap also deadlocks writeback against the folio it already holds locked. These files are maintained by the driver itself and have no valid reason to be written through the file interface. Mark base metadata files (mft_no < FILE_first_user) as immutable during inode read so the VFS rejects write, mmap, truncate and unlink with -EPERM. Directories are skipped so the root and \$Extend remain usable. Internal metadata updates do not go through the VFS write path and are unaffected.	2026-08-15	9.1	CVE-2026-72186
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: sanitize MFT references returned from ntfs_lookup_inode_by_name() ntfs_lookup_inode_by_name() returns MFT references read from directory index entries on disk. These values are untrusted, but the function can currently return an error-marked MFT reference to its callers without validating it. Callers later decode lookup failures with MREF_ERR(). A crafted NTFS image can set the MREF error bit while leaving the low bits as an arbitrary value, causing callers to consume a bogus pseudo-errno instead of treating the lookup result as corrupted on-disk metadata. Fix this at the source by normalizing every error-marked MFT reference returned from ntfs_lookup_inode_by_name() to ERR_MREF(-EIO). Apply this to all four directory lookup return paths so every caller gets a validated result without needing additional checks or an API change. This keeps the sanitization in the common lookup helper, which is cleaner than duplicating validation in each caller.	2026-08-15	9.1	CVE-2026-72188
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs3: validate split-point offset in indx_insert_into_buffer indx_insert_into_buffer() computes used = used1 - to_copy - sp_size; memmove(de_t, Add2Ptr(sp, sp_size), used - le32_to_cpu(hdr1->de_off)); where sp and sp_size come from hdr_find_split(). hdr_find_split() walks entries by le16_to_cpu(e->size) without validating that each step stays within hdr->used or that the size field is at least sizeof(struct NTFS_DE). index_hdr_check(), the on-load gatekeeper, only validates header-level fields (used, total, de_off) and does not walk per-entry sizes. A crafted NTFS image whose leaf INDEX_HDR reports used == total but contains one interior NTFS_DE with size = 0xFFFF0 therefore passes validation, descends to indx_insert_into_buffer() through the ntfs_create() -> indx_insert_entry() path, and makes hdr_find_split() return an sp whose sp_size (0xFFFF0) greatly exceeds the remaining bytes in the buffer. The u32 subtraction underflows and the memmove count becomes a near-4-GiB value, producing an out-of-bounds kernel write that corrupts adjacent allocations and panics the kernel. Reproduced on 7.0.0-rc7 with UML + KASAN via a crafted image and a single 'touch' inside the mounted directory; crash site resolves to fs/ntfs3/index.c at the memmove. Trigger requires only local mount of an attacker-supplied filesystem image (USB, loopback, or removable media auto-mount). Reject the split whenever the chosen sp plus its declared size already extends past hdr1->used. This is the minimal fix; it preserves the existing hdr_find_split() contract and relies on the same out: cleanup path as the pre-existing error returns. A prior OOB read in the very same indx_insert_into_buffer() memmove was fixed in commit b8c44949044e ("fs/ntfs3: Fix OOB read in indx_insert_into_buffer") by tightening hdr_find_e(), but that fix does not cover the split-point size field path addressed here: sp is returned by hdr_find_split(), not hdr_find_e(), and the underflow is driven by sp->size rather than hdr->used exceeding hdr->total.	2026-08-15	9.8	CVE-2026-72191
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs3: bound to_move in indx_insert_into_root before hdr_insert_head indx_insert_into_root() promotes a full resident \$INDEX_ROOT into \$INDEX_ALLOCATION and copies all	2026-08-15	9.8	CVE-2026-72192

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	non-last resident root entries into a newly allocated INDEX_BUFFER via <code>hdr_insert_head()</code> . The source byte count 'to_move' is summed from the on-disk resident entry sizes and is independent of the destination buffer size, which comes from <code>root->index_block_size</code> (via <code>indx->index_bits</code>). A crafted NTFS image that keeps a valid, full resident root but shrinks <code>root->index_block_size</code> down to 512 after the root has been populated makes <code>hdr_insert_head()</code> memcpy attacker-controlled resident entry bytes past the end of the <code>kmallocc(1u << indx->index_bits)</code> allocation returned by <code>indx_new()</code> . For a 512-byte destination and a resident root whose non-last entries total 560 bytes, the memcpy overruns by 120 bytes and a following memmove extends the highest written offset to 136 bytes past the allocation. The overflow bytes are a direct copy of on-disk entries (via <code>kmemdup</code>), so they are fully attacker-controlled. The write is reachable from unprivileged <code>open(O_CREAT)</code> on a mounted crafted NTFS image: a single sufficiently long create in a directory whose resident root is already full forces root promotion and triggers the copy. This is a controlled out-of-bounds write of 120-136 bytes past a <code>kmallocc(index_block_size)</code> allocation, with attacker-controlled content. It is a bounded adjacent-heap corruption primitive; it is not an arbitrary-address write. Successful exploitation into a named victim object depends on the surrounding slab layout. Reject the copy at the sink. The destination's INDEX_HDR already reports <code>hdr_total</code> (the payload capacity of the new buffer) and <code>hdr_used</code> (the bytes already consumed by the terminal END entry installed by <code>indx_new()</code>); require that <code>to_move</code> fits in the remaining payload before calling <code>hdr_insert_head()</code> . On mismatch, fail with <code>-EINVAL</code> and mark the filesystem as having a detected on-disk inconsistency, which is the same behaviour as the surrounding validation in this function.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>fs/ntfs3</code> : add depth limit to <code>indx_find_buffer</code> to prevent stack overflow <code>indx_find_buffer()</code> recursively descends the B+ tree index with no depth limit. A crafted NTFS image with circular index node references causes unbounded recursion, overflowing the kernel stack and panicking the system. This is reachable by mounting a malicious NTFS filesystem (e.g. from a USB drive via desktop automount) and deleting a file whose index entry triggers the rebalancing fallback path in <code>indx_delete_entry()</code> . Add a depth parameter and bail out with <code>-EINVAL</code> when it reaches the <code>fnid->nodes</code> array bound, matching the constraint already enforced by <code>fnid_push()</code> in <code>indx_find()</code> . The related function <code>indx_find()</code> was previously patched for a similar infinite-loop issue (commit 1732053c8a6b), but <code>indx_find_buffer()</code> was missed.	2026-08-15	9.8	CVE-2026-72194
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>ntfs</code> : validate resident index root values on lookup Resident <code>\$INDEX_ROOT</code> values carry index header fields that callers consume after lookup. Some callers already validate parts of the layout before walking entries, but those checks are scattered and do not cover all root header invariants, such as <code>entries_offset</code> alignment and lower bound, <code>index_length</code> , and <code>allocated_size</code> consistency. The resident root resize paths now keep these header fields consistent while the value size changes: <code>ntfs_ir_truncate()</code> lowers <code>index.allocated_size</code> before shrinking the resident value, and <code>ntfs_ir_reparent()</code> grows the resident value before publishing a larger root header. Lookup-time validation can therefore cover these invariants without tripping over the driver's own resize paths. Add <code>\$INDEX_ROOT</code> to the minimum resident value size table and validate the resident index header fields before returning the attribute from lookup. Require 8-byte aligned index header fields, a sane <code>entries_offset</code> , an <code>index_length</code> within <code>allocated_size</code> , <code>allocated_size</code> within the resident value, and enough entry space for at least an index entry header. The shared validator already rejects non-resident records for resident-only attribute types, including <code>\$INDEX_ROOT</code> .	2026-08-15	9.8	CVE-2026-72199
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>ntfs</code> : detect mapping-pairs LCN accumulator overflow The NTFS mapping-pairs parser accumulates relative LCN deltas in a signed integer. A corrupted attribute can drive that addition past the representable range. One corrupt runlist shape sets the accumulated LCN to <code>S64_MAX</code> and then adds a delta of 1 in the next mapping-pairs entry. Signed overflow is undefined and can turn an invalid runlist into a different set of physical clusters. Check the LCN addition for overflow before storing the next run.	2026-08-15	9.8	CVE-2026-72200
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>ntfs</code> : validate index entries on reading Validate index entries immediately after reading an index root or index block from disk. This eliminates repeated checks in lookup and <code>readdir</code> , and reduce the risk of missing checks in those paths.	2026-08-15	9.8	CVE-2026-72201

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: validate index block header more strictly Modify ntfs_index_block_inconsistent() to perform stricter validation of INDEX_HEADER geometry in INDX blocks, and update ntfs_lookup_inode_by_name() to use that function to validate INDX blocks.	2026-08-15	9.8	CVE-2026-72206
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: not change 0-byte \$DATA attribute to non-resident When ntfs_resident_attr_resize() cannot grow a resident attribute in place, it retries after converting other resident attributes to non-resident to free space in the MFT record. Do not select zero-length resident \$DATA attributes for this conversion. fsck treats 0-byte non-resident \$DATA attribute as corruptions.	2026-08-15	9.8	CVE-2026-72207
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: add bounds check before accessing EA entries in ntfs_ea_lookup and ntfs_listxattr, this verifies that there is enough space in the EA entry before accessing the next_entry_offset field of the EA entry.	2026-08-15	9.8	CVE-2026-72208
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: validate attribute values on lookup ntfs_attr_find() and ntfs_external_attr_find() check that generic resident attribute values fit in their attribute records and that fixed-size resident values are large enough. For variable-length resident formats, however, the fixed part is not enough: embedded length fields can still point callers past the resident value. A crafted image can set a small resident \$FILE_NAME value_length while leaving file_name_length large. Callers then trust file_name_length and read past the resident value when converting or comparing the name. This was reproduced with a crafted image under KASAN as a slab-out-of-bounds read from the kmalloc-1k MFT record copy. The stack included ntfs_lookup(), ntfs_iget(), ntfs_read_locked_inode(), ntfs_attr_name_get(), ntfs_ucstons(), and utf16s_to_utf8s(). Add a shared attribute value validator and use it before a lookup path can return an attribute, including the AT_UNUSED enumeration case where callers inspect returned attributes directly. The helper validates resident value bounds, minimum resident value sizes, variable-length \$FILE_NAME fields, and non-resident mapping-pairs metadata that was previously checked separately in both lookup paths. This also preserves the intended resident @val matching semantics in the external attribute lookup path. The old duplicated validation block overwrote the actual resident value length with the type-specific minimum length before comparing @val, so variable-length resident values could fail to match even when the bytes were identical. Keep the comparison on the actual value length, and make ntfs_attrlist_entry_add() compare resident attributes with lowest_vcn zero instead of reading the non-resident union member after a successful resident match. Reject non-resident \$FILE_NAME records too: the format requires \$FILE_NAME to be resident and callers treat returned records as resident.	2026-08-15	9.8	CVE-2026-72209
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: fix off-by-one in mapping pairs decoding bounds checks In ntfs_mapping_pairs_decompress(), attr_end points one byte past the end of the attribute record: attr_end = (u8 *)attr + le32_to_cpu(attr->length); The two bounds checks validating that mapping pair data bytes fit within the attribute use strict greater-than (>), which allows a one-byte out-of-bounds read when the data extends exactly to attr_end: b = *buf & 0xf; if (b) { if (unlikely(buf + b > attr_end)) // off-by-one goto io_error; for (deltaxcn = (s8)buf[b--]; b; b--) deltaxcn = (deltaxcn << 8) + buf[b]; } When buf + b == attr_end, the check evaluates to false and buf[b] reads one byte past the valid attribute boundary. The same pattern appears in the LCN delta bytes check. Fix both checks to use >= so that buf[b] at exactly attr_end is correctly rejected as out of bounds.	2026-08-15	9.8	CVE-2026-72210
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: grow index root value before reparent header update ntfs_ir_reparent() moves the resident index root entries into an index block and leaves a small root stub containing the child VCN. That root stub can be larger than the existing resident value. For example, an empty root with value_length 48 has an index area of 32 bytes, while the large-index root stub needs index_length and allocated_size of 40 bytes. The current code publishes the larger index.index_length and index.allocated_size before resizing the resident value. If the resize returns -ENOSPC, the recovery path can call ntfs_inode_add_attrlist(), which looks attributes up again while the root header says allocated_size 40 but the resident value still only provides 32 bytes of index area. Lookup-time \$INDEX_ROOT validation then correctly rejects that transient layout as corrupt. This reproduces as a generic/013 failure under qemu. In the failing run, the transient root had value_len=48, index_size=32, index_length=40, and allocated_size=40, and ntfsprogs-plus ntfsck reported	2026-08-15	9.8	CVE-2026-72211

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	"Corrupt index root in MFT record 1177". When the root stub grows, resize the resident value before publishing the larger root header. If the resize fails, the old root remains valid for recovery lookups. Keep the existing header-before-resize ordering for shrink or same-size cases so the resident value never temporarily exposes an allocated_size beyond its bounds.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Bound-check xdr_buf_to_bvec() stores before writing xdr_buf_to_bvec() writes a bio_vec into the caller's array before testing whether that slot is in range, and the head branch performs the store with no check at all. When the caller's budget is exactly used up, the next store lands one element past the end of the array. The overflow label returns count - 1, which masks the surplus store but cannot undo it. rq_bvec, the array passed by nfsd_vfs_write(), is allocated to exactly rq_maxpages entries with no slack. The OOB store can land in adjacent slab memory; the bv_len and bv_offset fields written there are derived from client-supplied RPC payload sizes. Move the in-range check ahead of the store in the head, page-loop, and tail branches. With the check at the top of each sequence, count is incremented only after a successful store, so the overflow label can return count directly.	2026-08-15	9.8	CVE-2026-72217
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sunrpc: harden rq_procinfo lifecycle to prevent double-free The svc_release_rqstp() function executes the callback inside rqstp->rq_procinfo->pc_release. However, if a worker thread begins processing a new request and encounters an early error path (e.g., unsupported protocol, short frame, or bad auth) before a valid rq_procinfo is installed, a stale release hook can be re-triggered against reused state from the previous RPC, resulting in a double-free or use-after-free vulnerability. Harden the lifecycle of rq_procinfo by: 1. Ensuring svc_release_rqstp() always clears rq_procinfo after the optional pc_release() call, regardless of whether the hook exists. 2. Explicitly clearing rq_procinfo at request entry in svc_process() before any early decode or drop paths. 3. Ensuring svc_process_bc() does the same at backchannel entry. This guarantees that error flows will not encounter a non-NULL stale rq_procinfo pointer when there is nothing to release.	2026-08-15	9.8	CVE-2026-72220
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sunrpc: wait for in-flight TLS handshake callback when cancel loses race When wait_for_completion_interruptible_timeout() in svc_tcp_handshake() returns 0 (timeout) or -ERESTARTSYS (signal) and tls_handshake_cancel() then returns false, handshake_complete() has won the cancellation race: it has set HANDSHAKE_F_REQ_COMPLETED and is about to invoke svc_tcp_handshake_done(), but the callback's side effects on xpt_flags and on svsk->sk_handshake_done have not yet committed. The current code reads xpt_flags immediately to decide whether the session succeeded. Two races result. If the callback has executed set_bit(XPT_TLS_SESSION) but not yet clear_bit(XPT_HANDSHAKE), svc_tcp_handshake() sees a session, enqueues the transport, and returns. svc_xprt_received() then clears XPT_BUSY, a worker thread picks the transport up, the dispatcher in svc_handle_xprt() observes XPT_HANDSHAKE still set, and xpo_handshake is invoked a second time. That svc_tcp_handshake() calls init_completion(&svsk->sk_handshake_done) while the original callback concurrently calls complete_all() on it, corrupting the embedded swait_queue. If the callback has set HANDSHAKE_F_REQ_COMPLETED but not yet entered svc_tcp_handshake_done(), svc_tcp_handshake() reads XPT_TLS_SESSION as clear and tears the connection down even though the handshake is about to succeed. Wait for the callback to commit before inspecting xpt_flags. The completion is guaranteed to fire because handshake_complete() invokes svc_tcp_handshake_done() unconditionally once it has set HANDSHAKE_F_REQ_COMPLETED.	2026-08-15	9.8	CVE-2026-72221
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sunrpc: pin svc_xprt across the asynchronous TLS handshake callback svc_tcp_handshake() stores the raw svc_xprt pointer in tls_handshake_args.ta_data and submits the request through tls_server_hello_x509(). The handshake core takes only sock_hold(req->hr_sk); nothing references the embedding struct svc_sock that svc_tcp_handshake_done() reaches via container_of(). Two close races leave the in-flight callback writing through a freed svc_sock. svc_sock_free() calls tls_handshake_cancel() and discards its return value: a false return means handshake_complete() has already set HANDSHAKE_F_REQ_COMPLETED but hp_done() may not have finished, yet svc_sock_free() proceeds to kfree(svsk). The cancel-loser fall-through inside svc_tcp_handshake() itself produces the same window: when wait_for_completion_interruptible_timeout() returns <= 0 (timeout	2026-08-15	9.8	CVE-2026-72222

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	or signal) and <code>tls_handshake_cancel()</code> returns false, the function does not drain, returns, and <code>svc_handle_xprt()</code> calls <code>svc_xprt_received()</code> , which clears <code>XPT_BUSY</code> and can drop the last reference. A concurrent close then runs <code>svc_sock_free()</code> while <code>svc_tcp_handshake_done()</code> is still updating <code>xpt_flags</code> and walking <code>svsk->sk_handshake_done</code> . The corruption surfaces as <code>set_bit/clear_bit</code> RMW into the freed <code>xpt_flags</code> slab slot and as <code>complete_all()</code> walking and writing the freed <code>wait_queue_head_t</code> list embedded in <code>sk_handshake_done</code> -- a slab-corruption primitive, not a benign read. The path is reachable on any TLS-enabled NFS server whenever a connection close overlaps the <code>tlshd</code> downcall delivery window; the interruptible wait means signal delivery suffices, not just <code>SVC_HANDSHAKE_TO_EXPIRY</code> . Take <code>svc_xprt_get(xprt)</code> immediately before <code>tls_server_hello_x509()</code> so the in-flight callback owns its own reference. Release it on the two edges where the callback is guaranteed not to fire -- submission failure from <code>tls_server_hello_x509()</code> and a successful <code>tls_handshake_cancel()</code> -- and at the tail of <code>svc_tcp_handshake_done()</code> after <code>complete_all()</code> . [cel: rewrote commit message to describe the actual change]			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: tt: prevent TVLV OOB check overflow A TT unicast TVLV contains the number of VLANs stored in it. This number is an u16 and gets multiplied by the size of the struct <code>batadv_tvlv_tt_vlan_data</code> (8 bytes). The size can therefore overflow the u16 used to store the <code>tt_vlan_len</code> . All additional safety checks to prevent out-of-bounds access of the TVLV buffer are invalid due to this overflow. Using <code>size_t</code> prevents this overflow and ensures that the safety checks compare against the actual buffer requirements.	2026-08-15	9.8	CVE-2026-72226
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: access unicast_ttvn skb->data only after skb realloc The <code>pskb_may_pull()</code> called by <code>batadv_get_vid()</code> could reallocate the buffer behind the skb. Variables which were pointing to the old buffer need to be reassigned to avoid an use-after-free. This was done correctly for the ethernet header but missed for the unicast_packet pointer.	2026-08-15	9.8	CVE-2026-72234
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: x86/virt/sev: Revert "Drop WBINVD before setting MSR_AMD64_SYSCFG_SNP_EN" Revert 99cf1fb58e68 ("x86/virt/sev: Drop WBINVD before setting MSR_AMD64_SYSCFG_SNP_EN"). Section 8.8 of the SNP spec says: Before invoking <code>SNP_INIT_EX</code> with <code>INIT_RMP</code> set to 1, software must ensure that no CPUs contain dirty cache lines for the memory containing the RMP. Cachelines can be moved from cache to cache in a dirty state. The <code>wbinvd_on_all_cpus()</code> before <code>SNP_INIT_EX</code> flushes the caches for each CPU, but if the IPIs for WBINVD race with this dirty cacheline movement, it is possible that they may not get flushed, violating the firmware requirement. Doing <code>wbinvd_on_all_cpus()</code> before setting <code>SNPEn</code> is safer since the RMP table is not yet in use. [Heroically bisected by Srikanth.] [bp: Massage commit message.]	2026-08-15	9.3	CVE-2026-72239
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: support IPIP tunnel with direct xmit The combination of IPIP tunnel with direct xmit, eg. bridge device, breaks because no <code>dst_entry</code> is provided to check the skb headroom and to set the <code>iph->frag_off</code> field. This leads to invalid <code>dst</code> usage and can trigger a crash in the tunnel transmit path. Fix this by moving <code>dst_cache</code> and <code>dst_cookie</code> out of the runtime union so that they can be shared by neighbour, xfrm, and direct tunnel flows. For <code>FLOW_OFFLOAD_XMIT_DIRECT</code> tuples carrying tunnel metadata, preserve route state in these shared fields and release it through the common <code>dst</code> release path. Since <code>dst_entry</code> is now available to the three supported xmit modes and <code>dst_release()</code> already deals with NULL <code>dst</code> , remove the xmit type check in <code>nft_flow_dst_release()</code> . Moreover, skip the check if the <code>dst</code> entry is NULL in <code>nf_flow_dst_check()</code> which is now the case for the direct xmit case. Based on patch from Rein Wei <n05ec@lzu.edu.cn>.	2026-08-15	9.8	CVE-2026-72248
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: use dst in this direction when pushing IPIP header When pushing the IPIP header, the route of the other direction is used to calculate the headroom, use the route in this direction. Accessing the other tuple to set the IP source and destination is fine because this tuple does not provide such information to avoid storing redundant information. However, this tuple already provides the <code>dst</code> for this direction, this went unnoticed because this bug affects headroom and <code>iph->frag_off</code> only at this stage.	2026-08-15	9.8	CVE-2026-72249

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_nat_sip: reload possible stale data pointer quoting sashiko: ----- [...] noticed a potential memory bug and header corruption involving the SIP NAT helper. In net/netfilter/nf_nat_sip.c:nf_nat_sip(): if (skb_ensure_writable(skb, skb->len)) { nf_ct_helper_log(skb, ct, "cannot mangle packet"); return NF_DROP; } uh = (void *)skb->data + protoff; uh->dest = ct_sip_info->forced_dport; if (!nf_nat_mangle_udp_packet(skb, ct, ctinfo, protoff, 0, 0, NULL, 0)) { If a cloned or fragmented SKB is reallocated by skb_ensure_writable(), the old data buffer is freed. However, nf_nat_sip() fails to update *dptr to point to the new buffer. It also appears to use nf_nat_mangle_udp_packet() on what could be a TCP packet, which would overwrite the sequence number with a checksum update. ----- nf_conntrack_sip linerizes skbs, hence no fragmented skb can be seen. But clones are possible, so rebuild dptr. Disable nf_nat_mangle_udp_packet() branch for TCP streams. It doesn't look like this can ever happen, else we should have received bug reports about this, so just check the conntrack is UDP and drop otherwise. The calling conntrack_sip set ->forced_dport for SIP_HDR_VIA_UDP messages, so I don't think this is ever expected to be true for a TCP stream.	2026-08-15	9.8	CVE-2026-72251
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Inject SEA if guest VNCR isn't normal memory When constructing an L1 VNCR mapping, KVM unconditionally uses cacheable memory attributes, even if the underlying PFN isn't memory. This gets particularly hairy if the endpoint doesn't support cacheable memory attributes, potentially throwing an SError on writeback... While KVM does permit cacheable memory attributes on certain PFNMAP VMAs, kvm_translate_vnchr() isn't currently grabbing the VMA. So do the simpler thing for now and just reject everything that isn't memory.	2026-08-15	9.3	CVE-2026-72277
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Re-translate VNCR before injecting abort KVM faults in the VNCR page with FOLL_WRITE whenever the guest aborts for a write, similar to how a regular stage-2 mapping is handled. It is entirely possible that the guest reads from the VNCR before writing to it, in which case the PFN could only be read-only. Invalidate the VNCR TLB and re-fetch the translation upon taking a VNCR abort, allowing the host mapping to be faulted in for write the second time around. Interestingly enough, this also satisfies the ordering requirements of FEAT_ETLS2/3 between descriptor updates and MMU faults.	2026-08-15	9.3	CVE-2026-72278
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Respect read-only PFN when mapping L1 VNCR KVM currently maps the L1 VNCR into the host stage-1 by relying entirely on the permissions of the guest stage-1. At the same time, it is entirely possible that the backing PFN is read-only (e.g. RO memslot), meaning that the L1 VNCR should use at most a read-only mapping. Cache the writability of the PFN in the VNCR TLB and use it to constrain the resulting fixmap permissions. Promote VNCR permission faults to an SEA in the case where the guest attempts to write to a read-only endpoint. Conveniently, this also plugs a page leak found by Sashiko [*] resulting from the early return for a read-only PFN.	2026-08-15	9	CVE-2026-72279
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic: Handle race between interrupt affinity change and LPI disabling Hyunwoo Kim reports some really bad races should the following situation occur: - LPI-I is pending in vcpu-B's AP list - vcpu-A writes to vcpu-B's RD to disable its LPIs - vcpu-C moves I from B to C If the last two race nicely enough, vgic_prune_ap_list() can drop the irq and AP list locks, reacquire them, and in the interval the irq has been freed. UAF follows. The fix is two-fold: - Before dropping the irq and ap_list locks, take a reference on the irq - Do not try to handle migration of the pending bit: there is no expectation that this state is retained, as per the architecture With that, we're sure that the interrupt is still around, and we safely remove it from the AP list as it has no target at this stage (unless another interrupt fires, but that's another story).	2026-08-15	9.3	CVE-2026-72288
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic: Check the interrupt is still ours before migrating it vgic_prune_ap_list() drops both ap_list_lock and irq_lock while migrating an interrupt to another vCPU. After reacquiring the locks it only checks that the affinity is unchanged (target_vcpu == vgic_target_oracle(irq)) before moving the interrupt, which assumes that an interrupt whose affinity is preserved is still queued on this vCPU's ap_list. That assumption no longer holds if the interrupt is taken off the ap_list while the locks	2026-08-15	9.3	CVE-2026-72289

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	are dropped. vgif_flush_pending_lpis() removes the interrupt from the list and sets irq->vcpu to NULL, but leaves enabled/pending/target_vcpu untouched. As the interrupt is still enabled and pending, vgif_target_oracle() returns the same target_vcpu, so the affinity check passes and list_del() is run a second time on an entry that has already been removed. Also check that the interrupt is still assigned to this vCPU (irq->vcpu == vcpu) before moving it.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: Fix unlikely race in try_get_locked_pte() Fix an unlikely race in try_get_locked_pte(), which could have happened if puds or pmuds get unmapped between the p?dp_get() and p?d_offset() functions.	2026-08-15	9.3	CVE-2026-72291
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ife: require ETH_HLEN to be pullable in ife_decode() ife decode may return after making only the outer IFE header and metadata pullable. The caller then passes the decapsulated packet to eth_type_trans(), which expects the inner Ethernet header to be accessible from the linear data area. With a malformed IFE frame, the inner Ethernet header may still be shorter than ETH_HLEN in the linear area, which can lead to a crash in the original code. Fix this by extending the pull check in ife_decode() so that the inner Ethernet header is also guaranteed to be pullable before returning.	2026-08-15	9.1	CVE-2026-72296
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: restrict socket queue dumps in enqueue tracepoints tipc_sk_enqueue() runs with sk->sk_lock.slock held while the socket is owned by user context. The spinlock protects the backlog queue in this path, but it does not serialize against the socket owner consuming or purging sk_receive_queue. KASAN reported: CPU: 14 UID: 0 PID: 1050 Comm: tipc3 Not tainted 7.1.0-rc6+ #126 PREEMPT(lazy) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x76/0xa0 lib/dump_stack.c:123 print_report+0xce/0x5b0 mm/kasan/report.c:482 kasan_report+0xc6/0x100 mm/kasan/report.c:597 __asan_report_load4_noabort+0x14/0x30 mm/kasan/report_generic.c:380 tipc_skb_dump+0x1327/0x16f0 net/tipc/trace.c:73 tipc_list_dump+0x208/0x2e0 net/tipc/trace.c:187 tipc_sk_dump+0xaf6/0xd60 net/tipc/socket.c:3996 trace_event_raw_event_tipc_sk_class+0x312/0x5a0 net/tipc/trace.h:188 tipc_sk_rcv+0xb1d/0x1d50 net/tipc/socket.c:2497 tipc_node_xmit+0x1c3/0x1440 net/tipc/node.c:1689 __tipc_sendmsg+0x97a/0x1440 net/tipc/socket.c:1512 tipc_sendmsg+0x52/0x80 net/tipc/socket.c:1400 sock_sendmsg+0x2f6/0x3e0 net/socket.c:825 splice_to_socket+0x7f9/0x1010 fs/splice.c:884 do_splice+0xe21/0x2330 fs/splice.c:936 __do_splice+0x153/0x260 fs/splice.c:1431 __x64_sys_splice+0x150/0x230 fs/splice.c:1616 x64_sys_call+0xeb5/0x2790 arch/x86/entry/syscall_64.c:41 do_syscall_64+0xf3/0x620 arch/x86/entry/syscall_64.c:63 entry_SYSCALL_64_after_hwframe+0x76/0x7e arch/x86/entry/entry_64.S:130 RIP: 0033:0x71624e8aafe2 Code: 08 0f 85 71 3a ff ff 49 89 fb 48 89 f0 48 89 d7 48 89 ce 4c 89 c2 4d 89 ca 4c 8b 44 24 08 4c 8b 4c 24 10 4c 89 5c 24 08 0f 05 <c3> 66 2e 0f 1f 84 00 00 00 00 00 66 2e 0f 1f 84 00 00 00 00 66 RSP: 002b:0000716157ffed68 EFLAGS: 00000246 ORIG_RAX: 0000000000000113 RAX: ffffffffda RBX: 0000716157fff6c0 RCX: 000071624e8aafe2 RDX: 000000000000005f RSI: 0000000000000000 RDI: 0000000000000066 RBP: 0000716157ffed90 R08: 0000000000000800 R09: 0000000000000001 R10: 0000000000000000 R11: 0000000000000246 R12: ffffffff00 R13: 0000000000000021 R14: 0000000000000000 R15: 00007ff89799c40 </TASK> The TIPC_DUMP_ALL tracepoints in tipc_sk_enqueue() also dump sk_receive_queue and can therefore dereference skbs that the socket owner has already dequeued or freed. Restrict these dumps to TIPC_DUMP_SK_BKLGQ, which matches the queue protected by the held spinlock. Keep the change limited to the enqueue path, where the unsafe queue dump is reachable while the socket is owned by user context.	2026-08-15	9.8	CVE-2026-72299
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: pin upper rpc_clnt across the TLS connect_worker The TLS connect path has a use-after-free: nothing pins the upper rpc_clnt across the delayed connect_worker. xs_connect() stores task->tk_client in sock_xprt::clnt as a raw pointer and queues the worker; for TLS-secured transports that worker is xs_tcp_tls_setup_socket(), which reads several fields out of the saved pointer (cl_timeout, cl_program, cl_prog, cl_vers, cl_cred, cl_stats) to construct the args for the inner handshake rpc_clnt. The xprt does not reference the rpc_clnt; the rpc_clnt references the xprt. xs_destroy() does cancel the connect_worker, but it runs only when the xprt's	2026-08-15	9.8	CVE-2026-72317

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	refcount drops to zero, which cannot happen until the <code>rpc_clnt</code> releases its <code>cl_xprt</code> reference in <code>rpc_free_client_work()</code> . When a TLS handshake fails fatally (for example, an mTLS mount whose client cert does not match the server), the connecting task is woken with <code>-EACCES</code> and exits, the mount caller invokes <code>rpc_shutdown_client()</code> , and the upper <code>rpc_clnt</code> is freed before the queued <code>connect_worker</code> fires. <code>xs_tcp_tls_setup_socket()</code> then dereferences the freed <code>clnt</code> , producing the <code>refcount_t</code> underflow Michael Nemanov reported. Take a reference on the upper <code>rpc_clnt</code> in <code>xs_connect()</code> for TLS transports via a new <code>rpc_hold_client()</code> helper, and drop it in the <code>connect_worker</code> 's exit path with <code>rpc_release_client()</code> . The <code>xprt_lock_connect()</code> / <code>xprt_unlock_connect()</code> pairing already serialises <code>xs_connect()</code> with <code>xs_tcp_tls_setup_socket()</code> , so the take and release are balanced one-for-one. The non-TLS connect worker (<code>xs_tcp_setup_socket</code>) never reads <code>sock_xprt::clnt</code> , so leave that path alone and avoid the <code>clnt-holds-xprt-holds-clnt</code> cycle that would otherwise prevent <code>xprt</code> destruction.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: cifs: validate DFS referral string offsets <code>parse_dfs_referrals()</code> validates that the response header and referral array fit in the received buffer, but each referral also contains string offsets supplied by the server. Those offsets are used to compute the <code>DfsPath</code> and <code>NetworkAddress</code> string pointers without checking whether they still point inside the response buffer. A malformed referral can therefore make the computed pointer exceed the end of the buffer. The resulting negative <code>max_len</code> is then passed to <code>cifs_strndup_from_utf16()</code> , and the non-Unicode path forwards it to <code>kstrndup()</code> as a <code>size_t</code> , allowing <code>strlen()</code> to read out of bounds. Validate each string offset before deriving the string pointer.	2026-08-15	9.4	CVE-2026-72318
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: ensure inner headers in ICMP errors are in headroom Sashiko points out that after stripping the outer headers with <code>pskb_pull()</code> we should ensure the inner IP headers in ICMP errors from tunnels are present in the <code>skb</code> headroom for functions like <code>ipv4_update_pmtu()</code> , <code>icmp_send()</code> and <code>IP_VS_DBG()</code> . Also, add more checks for the length of the inner headers.	2026-08-15	9.8	CVE-2026-72319
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_lookup: fix catchall element handling with inverted lookups <code>nft_lookup_eval()</code> decides whether a lookup matched ('found') from the direct set lookup and <code>priv->invert</code> before falling back to the catchall element used by interval sets (e.g. <code>nft_set_rbtree</code>) for the open-ended default range. Since 'found' is never recomputed after 'ext' is replaced by the catchall lookup, inverted lookups (<code>NFT_LOOKUP_F_INV</code> , " <code>!= @set</code> ") can wrongly match or wrongly skip the catchall element, producing the wrong verdict. Fold the catchall lookup into 'ext' before computing 'found', matching the order already used by <code>nft_objref_map_eval()</code> .	2026-08-15	9.1	CVE-2026-72320
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: Fix potential UAF in MLD delayed work A race condition exists between device teardown and incoming MLD query processing, leading to a Use-After-Free in the MLD delayed work. During device destruction, the primary reference to <code>inet6_dev</code> is dropped, which can drop its refcount to 0. The actual freeing of <code>inet6_dev</code> memory is deferred via RCU. Concurrently, the packet receive path runs under RCU read lock and obtains the <code>inet6_dev</code> pointer. Because the memory is RCU-protected, CPU-0 can safely dereference <code>inet6_dev</code> even if its refcount has hit 0. However, if CPU-0 calls <code>igmp6_event_query()</code> and schedules delayed work, it attempts to acquire a reference using <code>in6_dev_hold()</code> . This increments the refcount from 0 to 1, triggering a "refcount_t: addition on 0" warning. Since the <code>inet6_dev</code> memory is still scheduled to be freed after the RCU grace period, the device is freed while the work is still scheduled. When the work runs, it accesses the freed memory, causing a kernel panic. Fix this by using <code>refcount_inc_not_zero()</code> (via a new helper <code>in6_dev_hold_safe()</code>) to prevent acquiring a reference if the device is already being destroyed. If the refcount is 0, we do not schedule the work.	2026-08-15	9.8	CVE-2026-72322
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv4: igmp: Fix potential UAF in <code>igmp_gq_start_timer()</code> A race condition exists between device teardown (<code>inetdev_destroy</code>) and incoming IGMP query processing (<code>igmp_rcv</code>), leading to a Use-After-Free in the IGMP timer callback. During device destruction, <code>inetdev_destroy()</code> drops the primary reference to <code>in_device</code> , which can drop its refcount to 0. The actual freeing of <code>in_device</code> memory is deferred via RCU (using <code>call_rcu()</code>). Concurrently, <code>igmp_rcv()</code> runs under RCU read lock and obtains the <code>in_device</code> pointer. Because the memory is RCU-protected, CPU-0 can safely dereference <code>in_device</code> even if its refcount has hit 0. However, if CPU-0 calls <code>igmp_gq_start_timer()</code> and re-arms the timer, it attempts to acquire a reference	2026-08-15	9.8	CVE-2026-72323

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	using in_dev_hold(). This increments the refcount from 0 to 1, triggering a "refcount_t: addition on 0" warning. Since the in_device memory is still scheduled to be freed after the RCU grace period (as the free callback does not check the refcount again), the device is freed while the timer is still armed. When the timer expires, it accesses the freed memory, causing a kernel panic. Fix this by using refcount_inc_not_zero() (via a new helper in_dev_hold_safe()) to prevent acquiring a reference if the device is already being destroyed. If the refcount is 0, we do not arm the timer. A similar issue in IPv6 MLD is fixed in a subsequent patch.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/liquidio: drop cached VF pci_dev LUT The PF SR-IOV enable path caches VF pci_dev pointers in dpiring_to_vfpcidev_lut[] by iterating with pci_get_device(). Those entries do not own a reference, because the iterator drops the previous device reference on each step. The cached pointer is then dereferenced later when handling OCTEON_VF_FLR_REQUEST. Replace the cached VF mapping with runtime lookup on the mailbox DPI ring: derive the VF index from q_no, resolve the VF via exported PCI IOV helpers, validate it with the PF pointer and VF ID, then issue pcie_flr() and drop the reference with pci_dev_put(). Remove the unused VF lookup table initialization and cleanup.	2026-08-15	9.3	CVE-2026-72329
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: qede: fix off-by-one in BD ring consumption on build_skb failure qede_rx_build_skb() and qede_tpa_rx_build_skb() do not check for a NULL return from qede_build_skb(). When it returns NULL under memory pressure, the functions still consume a BD from the ring before returning NULL. The callers then recycle additional BDs, resulting in one extra BD being consumed (off-by-one). This desynchronizes the BD ring, which can corrupt DMA page reference counts and lead to SLUB freelist corruption. Commit 4e910dbe3650 ("qede: confirm skb is allocated before using") added a NULL check inside qede_build_skb() to prevent a NULL pointer dereference, but did not address the missing NULL checks in the callers, making this off-by-one reachable. Fix this by adding NULL checks for the return value of qede_build_skb() in both qede_rx_build_skb() and qede_tpa_rx_build_skb(), returning NULL immediately before any BD ring manipulation.	2026-08-15	9.8	CVE-2026-72339
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: ip6tables: mark malformed IPv6 extension headers for hotdrop The ah, hbh and rt matches check that the fixed extension header is present, then use the header length field to derive the advertised extension header length for matching. For the ah match, add the missing advertised-length check. For hbh and rt, update the existing advertised-length checks. In all three cases, set hotdrop to true before returning false when the advertised extension header length exceeds the available skb data. Returning false treats the packet as a rule mismatch. Set hotdrop to true and drop malformed packets so they cannot bypass rules intended to drop packets with these IPv6 extension headers.	2026-08-15	9.1	CVE-2026-72348
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gue: validate REMCSUM private option length GUE private flags can indicate that remote checksum offload metadata is present. The private flags field itself is accounted for by guehdr_flags_len(), but guehdr_priv_flags_len() currently returns 0 even when GUE_PFLAG_REMCSUM is set. This lets a packet with only the private flags field pass validate_gue_flags(), after which gue_remcsum() and gue_gro_remcsum() read the missing REMCSUM start/offset fields from the following bytes. Account for GUE_PLEN_REMCSUM when GUE_PFLAG_REMCSUM is present so that malformed packets are rejected during option validation.	2026-08-15	9.8	CVE-2026-72351
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix barriering when walking subrequest list Fix the barriering used when walking the subrequest list in retry as there's a possibility of seeing a subreq that's just been added by the application thread.	2026-08-15	9.8	CVE-2026-72355
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix netfs_create_write_req() to handle async cache object creation netfs_create_write_req() will skip caching if the fscache cookie is disabled, but this is a problem because async cache object creation might not have got far enough yet that has been enabled - thereby causing the call to fscache_begin_write_operation() to be skipped. Fix this by removing the checks on the cookie and delegating this to fscache_begin_write_operation().	2026-08-15	9.8	CVE-2026-72366
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free of fp->owner.name in durable handle owner check Two concurrent SMB2 durable reconnects (DH2C/DHnC) on the same persistent_id race the fp-	2026-08-15	9.8	CVE-2026-72381

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	>owner.name compare-read in ksmbd_vfs_compare_durable_owner() against the kfree() in ksmbd_reopen_durable_fd()'s reopen-success path. fp->owner.name is a standalone kstrdup() buffer whose lifetime is independent of the fp refcount, and the two sites share no lock: the compare reads the buffer while the reopen frees it, so the strcmp() can dereference freed memory. Commit 7ce4fc40018d ("ksmbd: fix durable reconnect double-bind race in ksmbd_reopen_durable_fd") made the fp->conn claim atomic under global_ft.lock (closing the owner.name double-free and the ksmbd_file write-UAF), but the compare-read versus reopen-free pair was left unserialized. BUG: KASAN: slab-use-after-free in strcmp+0x2c/0x80 Read of size 1 by task kworker strcmp ksmbd_vfs_compare_durable_owner smb2_check_durable_oplock smb2_open Freed by task kworker: kfree ksmbd_reopen_durable_fd smb2_open Allocated by task kworker: kstrdup session_fd_check smb2_session_logoff The buggy address belongs to the cache kmalloc-8 Serialize both sides of the race with fp->f_lock. The global durable file-table lock still protects the durable reconnect claim, but fp->owner.name is per-open state and does not need to block unrelated durable table lookups or reconnects. The teardown is left at its existing location after the reopen-success point so that an __open_id() rollback still retains owner.name for a later legitimate reconnect to verify.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: eth: fbnic: don't cache shinfo across skb realloc fbnic_tx_iso() calls skb_cow_head() which may reallocate the skb including the shared info. We can't use the pointer calculated before the call. BUG: KASAN: slab-use-after-free in fbnic_tx_iso.isra.0+0x668/0x8e0 Read of size 4 at addr ff110000262edd98 by task swapper/5/0 Call Trace: fbnic_tx_iso.isra.0+0x668/0x8e0 fbnic_xmit_frame+0x622/0xba0 dev_hard_start_xmit+0xf4/0x620 Allocated by task 8653: __alloc_skb+0x11e/0x5f0 alloc_skb_with_frags+0xcc/0x6c0 sock_alloc_send_pskb+0x327/0x3f0 __ip_append_data+0x188b/0x47a0 ip_make_skb+0x24a/0x300 udp_sendmsg+0x14d2/0x21e0 Freed by task 0: kfree+0x123/0x5a0 pskb_expand_head+0x36c/0xfa0 fbnic_tx_iso.isra.0+0x500/0x8e0 fbnic_xmit_frame+0x622/0xba0 dev_hard_start_xmit+0xf4/0x620 sch_direct_xmit+0x25b/0x1100 The buggy address belongs to the object at ff110000262edc40 which belongs to the cache skbuff_small_head of size 640 The buggy address is located 344 bytes inside of freed 640-byte region [ff110000262edc40, ff110000262ede	2026-08-15	9.8	CVE-2026-72393
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: add INIT verification after cookie unpacking In SCTP handshake, the INIT chunk is initially processed by the server and embedded into the cookie carried in INIT-ACK. The client then returns this cookie via COOKIE-ECHO, where the server unpacks it and reconstructs the original INIT chunk. When cookie authentication is enabled, the cookie contents are protected against tampering, so reusing the unpacked INIT without re-verification is safe. However, when cookie authentication is disabled, the reconstructed INIT can no longer be trusted. In this case, the INIT must be explicitly validated after unpacking to avoid processing potentially tampered data. Add sctp_verify_init() checks after cookie unpacking in COOKIE-ECHO processing paths (sctp_sf_do_5_1D_ce() and sctp_sf_do_5_2_4_dupcook()) when cookie_auth_enable is disabled. On failure, the new association is freed and the packet is discarded. Also tighten cookie validation in sctp_unpack_cookie() by verifying the embedded chunk type is SCTP_CID_INIT before treating it as an INIT chunk. Finally, update sctp_verify_init() to validate parameter bounds using the actual embedded INIT length instead of chunk->chunk_end, since the INIT stored in COOKIE-ECHO may not span the entire chunk buffer.	2026-08-15	9.8	CVE-2026-72398
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: enetc: check the number of BDs needed for xdp_frame The size of xdp_redirect_arr array is ENETC_MAX_SKB_FRAGS. However, the number of fragments contained in xdp_frame may be greater than or equal to ENETC_MAX_SKB_FRAGS, which will cause the access to xdp_redirect_arr to be out of bounds.	2026-08-15	9.8	CVE-2026-72399
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/mm: Fix handling of _PAGE_UNUSED pte bit The _PAGE_UNUSED softbit should not really be lying around. Its sole purpose is to signal to try_to_unmap_one() and try_to_migrate_one() that the page can be discarded instead of being moved / swapped. KVM has no way to know why a page is being unmapped, so it sets the bit on userspace ptes corresponding to unused guest pages every time they get unmapped. KVM has no reasonable way to clear the bit once the page is in use again. While set_ptes() checks and clears the bit, other paths that set new ptes did	2026-08-15	9.3	CVE-2026-72412

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	not. This led to used pages being thrown out as if they were unused, causing guest corruption. Fix the issue by clearing the _PAGE_UNUSED bit for present ptes in set_pte(), i.e. whenever a present pte is getting set. The check in set_ptes() is then redundant and can be removed. Also fix gmap_helper_try_set_pte_unused() to only set the bit if the pte is present; the _PAGE_UNUSED bit is only defined for present ptes and thus should not be set for non-present ptes.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: Validate iph->ihl in nf_flow_ip4_tunnel_proto() Add sanity check for iph->ihl field in nf_flow_ip4_tunnel_proto() before using it to compute the header size, avoiding out-of-bounds access with malformed IP headers. While at it, use iph->protocol instead of the hardcoded IPPROTO_IP constant when setting ctx->tun.proto and reference ctx->tun.hdr_size when updating ctx->offset.	2026-08-15	9.8	CVE-2026-72417
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free of conn->preauth_info in concurrent SMB2 NEGOTIATE conn->preauth_info is shared connection state (struct preauth_integrity_info, kcalloc-96) that is allocated and freed by the SMB2 NEGOTIATE handler and read by the response send path. smb2_handle_negotiate() allocates conn->preauth_info, and on a deassemble_neg_contexts() failure kfree it and sets it to NULL. Both the allocation and the free/NULL happen under ksmbd_conn_lock(conn) (the connection srv_mutex), which is held across the whole handler body. The response send path smb3_preauth_hash_rsp(), called from the send: block of __handle_ksmbd_work(), reads conn->preauth_info and dereferences conn->preauth_info->Preauth_HashValue (via ksmbd_gen_preauth_integrity_hash()) without taking conn_lock. When a client drives two SMB2 NEGOTIATE requests on the same connection, one worker can free conn->preauth_info on the failing-negotiate path while a concurrent send-path worker is reading it, producing a slab use-after-free read (KASAN-confirmed). The send-path read tested conn->preauth_info for NULL but raced with the free that occurs between the NULL check and the dereference, so the NULL guard alone does not close the window. Serialize the NEGOTIATE-branch read in smb3_preauth_hash_rsp() under ksmbd_conn_lock(conn) and re-check conn->preauth_info inside the lock. Because the negotiate handler holds conn_lock across its kfree + NULL assignment, a reader that also takes conn_lock either runs fully before the allocation or fully after the NULL store, and can never observe the freed-but-not-yet-NULled pointer. ksmbd_gen_preauth_integrity_hash() takes no locks itself (it only computes a SHA-512 over the buffer), so no lock-ordering inversion is introduced, and conn_lock is a sleepable mutex which is safe on this send path (it already performs network I/O).	2026-08-15	9.8	CVE-2026-72422
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: ioam: fix type confusion of dst_entry IOAM uses a dummy dst_entry(null_dst) to mark that the destination should not be changed after the transformation. This dst is stored in the IOAM lwt state and may be passed to dst_cache_set_ip6(). However, the IPv6 dst cache path eventually calls rt6_get_cookie(), which treats the dst_entry as part of a struct rt6_info. Since the null_dst was embedded directly as a struct dst_entry in struct ioam6_lwt, this resulted in an invalid cast and rt6_get_cookie() reading fields from the wrong object. In practice, the wrong cookie is not used while rt->obsolete is zero, but rt6_get_cookie() may also access per-cpu value when rt->sernum aliases ioam6_lwt::cache::reset_ts, which can become zero, making this a potential invalid pointer access. Fix this by embedding a full struct rt6_info for the dummy IPv6 route and passing its dst member to the dst APIs.	2026-08-15	9.8	CVE-2026-72429
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: Don't use test_bit() in lockless RCU readers in hash types Sashiko pointed out that there are a few lockless RCU readers using test_bit() which is a relaxed atomic operation and provides no memory barrier guarantees. Use test_bit_acquire() instead where the operation may run parallel with add/del/gc, i.e. is not one from the next cases - protected by region lock - in a set destroy phase - in a new/temporary set creation phase	2026-08-15	9.8	CVE-2026-72436
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: fix and simplify IP6IP6 tunnel handling Fix nf_flow_ip6_tunnel_proto() to use pskb_may_pull() instead of skb_header_pointer() to ensure the outer IPv6 header is in the skb headroom, which is required for subsequent packet processing. Move ctx->offset update inside the IPPROTO_IPV6 conditional block since it should only be adjusted when an IP6IP6 tunnel is actually detected. Simplify the rx path by removing ipv6_skip_exthdr() and checking ip6h->nexthdr directly, as the flowtable fast path only handles simple IP6IP6 encapsulation	2026-08-15	9.8	CVE-2026-72442

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	without extension headers. Drop the tunnel encapsulation limit destination option support from the tx path to match, since the rx path no longer handles extension headers. Remove the encap_limit parameter from nf_flow_offload_ipv6_forward(), nf_flow_tunnel_ip6ip6_push() and nf_flow_tunnel_v6_push(), along with the ipv6_tel_txoption struct and related headroom/MTU adjustments.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: Fix xfrm state cache insertion race The xfrm input state cache insertion code checks the validity of the state before acquiring the global xfrm_state_lock. Thus it's possible for someone else to kill the state after it passed the validity check, and then the insertion will add the dead state to the cache. Fix this by moving the validity check inside the lock. This entire function is called on the input path, where BH must be off (e.g., the caller of this function xfrm_input acquires its spinlocks without disabling BH). So there is no need to disable BH here or take the RCU read lock. Remove both and replace them with an assertion that trips if BH is accidentally enabled on some future calling path.	2026-08-15	9.8	CVE-2026-72451
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: Fix dev use-after-free in xfrm async resumption xfrm async resumption hold skb->dev refcnt until after transport_finish. However, xfrm_rcv_cb may modify skb->dev to tunnel dev without taking device reference, such as vti_rcv_cb. The subsequent async resumption will decrement the tunnel device's reference count, which lead to uaf of tunnel dev and refcnt leak of orig dev as below: unregister_netdevice: waiting for vti1 to become free. Usage count = -2 Stash the original skb->dev to fix refcnt imbalance. The new skb->dev set by xfrm_rcv_cb can race with device teardown. Extend rcu protection over xfrm_rcv_cb and transport_finish to prevent races.	2026-08-15	9.8	CVE-2026-72463
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xprtrdma: Fix bcall rep leak and unbounded peek rpcrdma_is_bcall() decodes a reply's first words to decide whether the frame is a backchannel call. Two issues in that decode path let a short or malformed reply leak the receive buffer and drain the Receive queue. First, the speculative peek p = xdr_inline_decode(xdr, 0); /* five p++ reads follow */ asks xdr_inline_decode() for zero bytes, which returns xdr->p without consulting xdr->end. The five subsequent __be32 reads can then walk up to 20 bytes past the wire payload into stale regbuf contents and misclassify the reply as a backchannel call. Second, after the post-peek p = xdr_inline_decode(xdr, 3 * sizeof(*p)); if (unlikely(!p)) return true; the short-header arm returns true without calling rpcrdma_bc_receive_call(). The contract with the caller is that a true return transfers ownership of rep to the backchannel path: rpcrdma_reply_handler() if (rpcrdma_is_bcall(r_xprt, rep)) return; /* bare return, skips out_post */ ... out_post: rpcrdma_post_recvs(r_xprt, credits + ...); Because rpcrdma_bc_receive_call() never ran, no one took rep, but rpcrdma_reply_handler still bare-returns past rpcrdma_rep_put() and rpcrdma_post_recvs(). The rep, with its persistently DMA-mapped receive buffer, is orphaned on rb_all_reps and freed only at transport teardown. This completion reposts nothing, so its slot is reclaimed only when a later forward-channel reply reaches out_post and rpcrdma_post_recvs() allocates a fresh rep to backfill; absent that traffic the Receive queue drains and the peer's Sends draw RNR NAKs. Fix by consulting xdr->end after the zero-length peek so the five __be32 reads cannot run unless 20 bytes of wire payload remain. A byte-precise comparison against xdr->end is required because a non-4-aligned receive rounds the stream's word count up past the true payload. Also return false from the short-header arm so the reply falls through the normal out_norqst cleanup chain (rpcrdma_rep_put() plus rpcrdma_post_recvs()).	2026-08-15	9.8	CVE-2026-72466
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nfs: use nfsi->rwsem to protect traversal of the file lock list Lingfeng identified a bug and suggested two solutions, but both appear to have issues. Generally, we cannot release flc_lock while iterating over the file lock list to avoid use-after-free (UAF) problems with file locks. However, functions like nfs_delegation_claim_locks and nfs4_reclaim_locks cannot adhere to this rule because recover_lock or nfs4_lock_delegation_recall may take a long time. To resolve this, NFS switches to using nfsi->rwsem for the same protection, and nfs_reclaim_locks follows this approach. Although nfs_delegation_claim_locks uses so_delegreturn_mutex instead, this is inadequate since a single inode can have multiple nfs4_state instances. Therefore, the fix is to also use nfsi->rwsem in this case. Furthermore, after commit c69899a17ca4 ("NFsv4: Update of VFS byte range lock must be atomic with the stateid update"), the functions nfs4_locku_done and	2026-08-15	9.8	CVE-2026-72472

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	nfs4_lock_done also break this rule because they call locks_lock_inode_wait without holding nfsi->rwsem. Simply adding this protection could cause many deadlocks, so instead, the call to locks_lock_inode_wait is moved into _nfs4_proc_setlk. Regarding the bug fixed by commit c69899a17ca4 ("NFSv4: Update of VFS byte range lock must be atomic with the stateid update"), it has been resolved after commit 0460253913e5 ("NFSv4: nfs4_do_open() is incorrectly triggering state recovery") because all slots are drained before calling nfs4_do_reclaim, which prevents concurrent stateid changes along this path. Also, nfs_delegation_claim_locks does not cause this concurrency either since when _nfs4_proc_setlk is called with NFS_DELEGATED_STATE, no RPC is sent, so nfs4_lock_done is not called. Therefore, nfs4_lock_delegation_recall from nfs_delegation_claim_locks is the first time the stateid is set.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xprtrdma: Decouple req recycling from RPC completion rl_kref formerly served two distinct lifetimes through a single refcount: it gated when a Reply could wake its RPC task, and it gated when an rprcdma_req could return to its free pool. The marshal path took the Send-side reference only when SGEs needed DMA-unmap (sc_unmap_count > 0), which made a Send carrying only pre-registered buffers an exception: the Reply handler dropped rl_kref from 1 to 0 and freed the req while the HCA might still be DMA-reading from its send buffer. Give rl_kref a narrower job. The RPC layer takes one reference when slot allocation hands a req out. rprcdma_prepare_send_sges() takes a Send-side reference unconditionally after WR preparation succeeds. xprt_rdma_free_slot() and xprt_rdma_bc_free_rqst() drop the RPC-layer reference; rprcdma_sendctx_unmap() drops the Send-side reference. The req returns to its free pool only after both owners have signed off. The existing kref_init(&req->rl_kref) call in rprcdma_prepare_send_sges() is removed. Initialization moves to the slot-allocation paths (xprt_rdma_alloc_slot and rprcdma_bc_rqst_get), and the release callback re-arms rl_kref before the req returns to a free pool. A re-init in the marshal path would discard the RPC-layer reference that already exists on entry. Three invariants follow: - Any rprcdma_req held by an rpc_rqst has rl_kref >= 1. xprt_rdma_alloc_slot(), rprcdma_bc_rqst_get(), and the backlog-wake branch in xprt_rdma_alloc_slot() each kref_init rl_kref before publishing the req. Without this invariant, an RPC task that aborts between slot allocation and marshal (gss_refresh failure or signal during call_connect, for example) would drive xprt_release() -> xprt_rdma_free_slot() -> kref_put against a refcount of zero, saturating refcount_t and stranding the slot. - The Send-side reference is taken only after WR prep succeeds. A mapping failure in rprcdma_prepare_send_sges() runs rprcdma_sendctx_cancel(), which DMA-unmaps the sendctx and clears sc_req without touching rl_kref. The sendctx ring walks in rprcdma_sendctx_put_locked() and rprcdma_sendctxs_destroy() skip entries with sc_req == NULL, so a burst of -EIO marshal failures cannot hold reqs off rb_send_bufs. - The release callback re-arms rl_kref so the next consumer enters with the invariant satisfied. Replies now complete the RPC directly. rprcdma_reply_handler() calls rprcdma_complete_rqst() in place of kref_put on the non-LocalInv branch. The LocalInv branch already completes the RPC from frwr_unmap_async() and is unaffected. Because Send-side references can now outlive RPC completion, connection teardown drains sendctx entries whose unsigned Sends never had a later signaled completion to walk the ring. rprcdma_sendctxs_destroy() walks the active range and runs rprcdma_sendctx_unmap() on each entry with a non-NULL sc_req before the request buffers are reset, and is moved ahead of rprcdma_reqs_reset() in rprcdma_xprt_disconnect() so the reqs are still in their pre-reset state when the Send-side refs are released. The drain creates a teardown-ordering hazard on the backchannel path. With the new lifetime, releasing a bc_prealloc req from rprcdma_req_release() re-adds it to bc_pa_list. The disconnect in xprt_rdma_destroy() runs after xprt_destroy_backchannel() has already emptied bc_pa_list, so the drained reqs would otherwise leak. xprt_rdma_destroy() now runs xprt_rdma_bc_destroy(xprt, 0) a second time after the disconnect to reclaim them.	2026-08-15	9.8	CVE-2026-72473
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: call _ntfs_bad_inode() when failing to rename It is safe to call _ntfs_bad_inode on live inodes since: commit 519b078998ce ("fs/ntfs3: Exclude call make_bad_inode for live nodes.") The WARN_ON was added when it wasn't safe by: commit d99208b91933 ("fs/ntfs3: cangle set bad inode after removing name fails") Replace	2026-08-15	9.8	CVE-2026-72477

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the WARN_ON with a call to _ntfs_bad_inode() to prevent further operations on the inconsistent inode.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/9p: fix race condition on rdma->state in trans_rdma.c The rdma->state field is modified without holding req_lock in both recv_done() and p9_cm_event_handler(), while rdma_request() accesses the same field under the req_lock spinlock. This inconsistent locking creates a race condition: - recv_done() running in softirq completion context sets rdma->state = P9_RDMA_FLUSHING without acquiring req_lock - p9_cm_event_handler() modifies rdma->state at multiple points (ADDR_RESOLVED, ROUTE_RESOLVED, ESTABLISHED, CLOSED) without req_lock - rdma_request() uses spin_lock_irqsave(&rdma->req_lock, flags) to protect the read-modify-write of rdma->state The race can cause lost state transitions: recv_done() or the CM event handler could set state to FLUSHING/CLOSED while rdma_request() is concurrently checking or modifying state under the lock, leading to the FLUSHING transition being silently overwritten by CLOSING. This corrupts the connection state machine and can cause use-after-free on RDMA request objects during teardown. Fix by adding req_lock protection to all rdma->state modifications in recv_done() and p9_cm_event_handler(), matching the pattern already used in rdma_request(). Use spin_lock_irqsave/spin_unlock_irqrestore in the CM event handler since it can race with recv_done() which runs in softirq context. Tested with a kernel module that races two threads (simulating rdma_request and recv_done/CM handler) on rdma->state with proper locking: 5.5M+ FLUSHING writes over 27M iterations with 0 lost transitions.	2026-08-15	9.8	CVE-2026-72491
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: serialize netif_running() check in enqueue_to_backlog() Syzbot reported a KASAN slab-use-after-free in fib_rules_lookup(). The root cause is a race condition where packets can escape the backlog flushing during device unregistration (e.g., during netns exit). Commit e9e4dd3267d0 ("net: do not process device backlog during unregistration") introduced a lockless netif_running() check in enqueue_to_backlog() to prevent queuing packets to an unregistering device. However, this creates a TOCTOU race window. A lockless transmitter (like veth_xmit) can pass the check before dev_close() clears IFF_UP. If the transmitter is then delayed, flush_all_backlogs() can run and finish before the transmitter grabs the backlog lock and queues the packet. The packet then escapes the flush and triggers UAF later when processed. Fix this by moving the netif_running() check inside the backlog lock. This serializes the check with the flush work (which also grabs the lock). We then either queue the packet before the flush runs (so it gets flushed), or check netif_running() after the flush/close completes (so it gets dropped).	2026-08-15	9.9	CVE-2026-72493
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Replace waitqueue and flag with completion The driver previously used a waitqueue along with an explicit request_done flag, but without proper barriers around request_done. An earlier patch by Gui-Dong Han <hanguidong02@gmail.com> attempted to fix this by adding the missing memory barriers. Rather than adding the barriers, this patch replaces the waitqueue+flag with a completion, which is designed for this exact purpose.	2026-08-15	9.8	CVE-2026-72494
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Avoid repeated requests to allocate WC pages Applications can request multiple WC pages for the same ucontext. As of now, only 1 WC page per ucontext is supported. Add a lock to avoid concurrent access and a check to fail repeated requests. Also, if the mmap entry insert fails for the WC, free the Doorbell page index mapped for the WC page.	2026-08-15	9.3	CVE-2026-72495
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Proper rollback if the ioremap fails bnxt_qplib_alloc_dpi returns success even if ioremap fails. Add the proper rollback when the ioremap fails and return -ENOMEM status.	2026-08-15	9.2	CVE-2026-72496
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: fix UAF in tipc_l2_send_msg() Syzbot reported a slab-use-after-free in ipvlan_hard_header() when called from tipc_l2_send_msg(). The root cause is that tipc_disable_l2_media() calls synchronize_net() while b->media_ptr is still valid. This allows concurrent RCU readers to obtain the device pointer after synchronize_net() has finished. The pointer is cleared later in bearer_disable(), but without any subsequent synchronization, allowing the device to be freed while still in use by readers. Fix this by clearing b->media_ptr in tipc_disable_l2_media()	2026-08-15	9.8	CVE-2026-74255

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	before calling synchronize_net(). This is safe to do now because the call order in bearer_disable() was reversed in 0d051bf93c06 ("tipc: make bearer packet filtering generic") to call tipc_node_delete_links() (which needs the pointer) before disable_media(). https://lore.kernel.org/netdev/6a2c1007.428ffe26.258b27.015d.GAE@google.com/T/#u			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_codel: Do not call qdisc_tree_reduce_backlog during peek before restoring qlen Whenever codel drops packets during peek, it calls qdisc_tree_reduce_backlog. An issue arises because it calls qdisc_tree_reduce_backlog before it reincrements the qlen. If qlen drops to zero, but peek returns an skb, the parent's qlen_notify callback will be executed even though codel still has 1 packet on the queue and, thus, will mistakenly deactivate the parent's class causing issues like a wild memory access when qfq has codel as a child: [36.339843][T370] Oops: general protection fault, probably for non-canonical address 0xfbd59c0000000024: 0000 [#1] SMP KASAN NOPTI [36.340408][T370] KASAN: maybe wild-memory-access in range [0xdead000000000120-0xdead000000000127] [36.340737][T370] CPU: 2 UID: 0 PID: 370 Comm: tc Not tainted 7.1.0-rc5-00287-g66e13b626592 #87 PREEMPT(full) [36.341113][T370] Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 [36.341357][T370] RIP: 0010:qfq_deactivate_agg (include/linux/list.h:1029 (discriminator 2) include/linux/list.h:1043 (discriminator 2) net/sched/sch_qfq.c:1369 (discriminator 2) net/sched/sch_qfq.c:1395 (discriminator 2)) sch_qfq [36.342221][T370] RSP: 0018:ffff8881100ef370 EFLAGS: 00010216 [36.342422][T370] RAX: 0000000000000000 RBX: ffff8881058a9568 RCX: dffffc0000000000 [36.342664][T370] RDX: 1ffff11021064dc3 RSI: ffff888108326e00 RDI: dffffc0000000000 [36.342905][T370] RBP: ffff8881058a8280 R08: dead000000000122 R09: 1bd5a00000000024 [36.343140][T370] R10: fffffbfff2940329 R11: fffffbfff2940329 R12: 0000000000000000 [36.343383][T370] R13: dead000000000100 R14: ffff8881058a9580 R15: ffff8881058a9578 [36.343631][T370] FS: 00007fc04b0ca780(0000) GS:ffff888184fef000(0000) knlGS:0000000000000000 [36.343911][T370] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [36.344116][T370] CR2: 0000557c02c02000 CR3: 000000010e0ba000 CR4: 0000000000750ef0 [36.344359][T370] PKRU: 55555554 [36.344481][T370] Call Trace: ... [36.345054][T370] qfq_reset_qdisc (net/sched/sch_qfq.c:357 net/sched/sch_qfq.c:1487) sch_qfq [36.345222][T370] qdisc_reset (net/sched/sch_generic.c:1057) [36.345503][T370] __qdisc_destroy (net/sched/sch_generic.c:1096) [36.345677][T370] qdisc_graft (net/sched/sch_api.c:1062 net/sched/sch_api.c:1053 net/sched/sch_api.c:1159) [36.346335][T370] tc_get_qdisc (net/sched/sch_api.c:1528 net/sched/sch_api.c:1556) Fix this by only calling qdisc_tree_reduce_backlog in peek after the qlen is restored.	2026-08-15	9.8	CVE-2026-74267
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: clear sock_ops cb flags before force-closing a child socket A child socket inherits the listener's bpf_sock_ops_cb_flags via sk_clone_lock(). If its setup fails in tcp_v4_syn_recv_sock() / tcp_v6_syn_recv_sock(), the child is freed through put_and_exit, where inet_csk_prepare_forced_close() drops the socket lock and tcp_done() runs without it. If BPF_SOCKET_OPS_STATE_CB_FLAG was inherited, tcp_done() -> tcp_set_state() calls tcp_call_bpf(), which expects the lock and trips sock_owned_by_me(): WARNING: include/net/sock.h:1799 at tcp_set_state+0x433/0x550 RIP: 0010:tcp_set_state+0x433/0x550 include/net/sock.h:1799 Call Trace: <IRQ> tcp_done+0xba/0x250 net/ipv4/tcp.c:5095 tcp_v4_syn_recv_sock+0x850/0xa50 net/ipv4/tcp_ipv4.c:1787 tcp_check_req+0xf30/0x1360 net/ipv4/tcp_minisocks.c:926 tcp_v4_rcv+0x1047/0x1b50 net/ipv4/tcp_ipv4.c:2164 </IRQ> The child is freed before it is ever established, so it should run no sock_ops callback. Clear its cb flags in inet_csk_prepare_for_destroy_sock(), the common point for the IPv4, IPv6 and chtls forced-close paths and for the MPTCP ->syn_recv_sock() failure path (dispose_child), which reaches tcp_done() on a child that was never established too.	2026-08-15	9.8	CVE-2026-74268
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bnxt: fix head underflow on XDP head-grow The xdp.py test test_xdp_native_adjst_head_grow_data crashes when run on a bnxt machine (and also crashes in NIPA). It seems that the bug is an underflow in bnxt_rx_multi_page_skb, which builds the skb head: napi_build_skb(data_ptr - bp->rx_offset, rxr->rx_page_size); The problem with this expression is that in page	2026-08-15	9.8	CVE-2026-74269

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mode, rx_offset is: bp->rx_offset = NET_IP_ALIGN + XDP_PACKET_HEADROOM; Which evaluates (at least on x86_64) to 258. The test test_xdp_native_adjst_head_grow_data tests a case where the head is adjusted by -256. When this test runs, data_ptr is shifted to frag_start + 2 (where frag_start = page_address(page) + offset). Then, bnxt_rx_multi_page_skb is invoked and the napi_build_skb expression subtracts 258, landing at an address before frag_start. This could be either the previous fragment or the previous physical page when the offset is < 256 (e.g. if the fragment started at offset 0). When the skb is freed, the page pool fragment reference is dropped on either the wrong page or the wrong frag of the right page. In either case, the corrupted reference count can lead to the page being prematurely recycled while still in use. Once (incorrectly) recycled, it can be handed out again and on driver teardown this would result in a double free. The commit under fixes updated this code to handle the case where the native page size is >= 64k, but it unintentionally broke the head grow case. To fix this, add an offset field to struct bnxt_sw_rx_bd, mirroring the existing offset field in struct bnxt_sw_rx_agg_bd. Populate it on allocation and preserve it on reuse. In bnxt_rx_multi_page_skb, use the newly added offset field to compute the fragment start and pass that to napi_build_skb. Adjust the layout with skb_reserve. There are two cases, the non-adjustment case and the adjustment case. In both cases, the skb is built at page_address(page) + offset to account for the case where the native page size >= 64K and skb_reserve is called with data_ptr - (page_address(page) + offset). That difference equals bp->rx_offset when data_ptr was not moved, or bp->rx_offset + xdp_adjust when XDP adjusted the head. Re-running the failing test with this commit applied causes the test to run successfully to completion. The other rx_skb_func implementations don't have this issue.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: validate embedded address parameter length sctp_verify_asconf() and sctp_verify_param() only validate ADD_IP, DEL_IP, and SET_PRIMARY parameters against a fixed minimum size of sizeof(struct sctp_addip_param) + sizeof(struct sctp_paramhdr). This ensures the outer parameter is large enough to contain an embedded address parameter header, but does not verify that the embedded address parameter's declared length fits within the bounds of the outer parameter. Later, sctp_process_param() and sctp_process_asconf_param() extract the embedded address parameter and pass it to af->from_addr_param(), which uses the address parameter length to parse the variable-length address payload. A malformed peer can therefore advertise an embedded address parameter length that exceeds the remaining bytes in the enclosing parameter. Validate that addr_param->p.length does not exceed the space available after the sctp_addip_param header before processing the embedded address parameter. Reject malformed parameters when the embedded address length extends beyond the enclosing parameter bounds. This prevents out-of-bounds reads when parsing malformed parameters carried in INIT or ASCONF processing paths.	2026-08-15	9.1	CVE-2026-74287
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vhost/net: complete zerocopy ubufs only once vhost-net initializes one ubuf_info per outstanding zerocopy TX descriptor and hands it to the backend socket. The networking stack may then clone a zerocopy skb before all skb references are released. For example, batman-adv fragmentation reaches skb_split(), which calls skb_zerocopy_clone() and increments the same ubuf_info refcount. vhost_zerocopy_complete() currently treats every ubuf callback as a completed vhost descriptor. It dereferences ubuf->ctx, writes the descriptor completion state, and drops the vhost_net_ubuf_ref even when the callback only releases a cloned skb reference. A backend reset can therefore wait for and free the vhost_net_ubuf_ref while another cloned skb still carries the same ubuf_info. A later completion then dereferences the freed ubufs pointer. KASAN reports the stale completion as: BUG: KASAN: slab-use-after-free in vhost_zerocopy_complete+0x1d7/0x1f0 BUG: KASAN: slab-use-after-free in vhost_zerocopy_complete+0x101/0x1f0 vhost_zerocopy_complete skb_copy_ubufs __dev_forward_skb2 veth_xmit The freed object was allocated from vhost_net_ioctl() while setting the backend and freed through kfree_rcu()/kvfree_rcu_bulk after backend removal, while delayed skb completion still reached vhost_zerocopy_complete(). Honor the generic ubuf_info refcount before touching vhost state, and run the vhost descriptor completion only for the final ubuf reference. This matches the msg_zerocopy_complete() ownership rule for cloned zerocopy skbs.	2026-08-15	9.3	CVE-2026-74310

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: lockd: Avoid hashing uninitialized bytes in nlm4svc_lookup_file() file_hash() digests the first LOCKD_FH_HASH_SIZE bytes of nfs_fh.data when bucketing nlm_files[], independent of fh.size. Commit 3de744ee4e45 ("lockd: Use xdrigen XDR functions for the NLMv4 TEST procedure") set .pc_argzero to zero for the converted procedures and moved file-handle population into nlm4svc_lookup_file(), which copies only xdr_lock->fh.len bytes into lock->fh.data. When an NLMv4 client presents a file handle shorter than LOCKD_FH_HASH_SIZE, bytes fh.len..31 retain whatever the argument buffer held from an earlier request. The same wire handle then hashes to different buckets across calls; nlm_lookup_file() misses the existing nlm_file entry, and lock-state lookups fail. Zero only the tail bytes that file_hash() would otherwise consume. Handles of LOCKD_FH_HASH_SIZE or larger already populate every byte that file_hash() reads.	2026-08-15	9.8	CVE-2026-74315
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/siw: Fix endpoint/socket association handling Disassociating a socket from an endpoint via siw_socket_disassoc() may release the last reference on that endpoint and free it. Therefore, don't clear the endpoints socket pointer after calling that function, but within. This fixes a: BUG: KASAN: slab-use-after-free in siw_cm_work_handler (drivers/infiniband/sw/siw/siw_cm.c:1053 drivers/infiniband/sw/siw/siw_cm.c:1075) which occurred after processing a malformed MPA request during connection establishment, causing the new endpoint to be closed.	2026-08-15	9.8	CVE-2026-74345
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: validate fast symlink target during inode read ocfs2_validate_inode_block() already rejects several inconsistent self-contained dinodes before they are exposed to the rest of the filesystem. Fast symlinks need the same treatment. A zero-cluster symlink is treated as a fast symlink and later read through page_get_link() and ocfs2_fast_symlink_read_folio(). That path uses strlen() on the inline payload and then copies len + 1 bytes into the folio. If a corrupt dinode stores an i_size that does not fit the inline area or omits the terminating NUL at i_size, that copy reads past the end of the inode block buffer. Reject zero-cluster symlink dinodes whose i_size exceeds the inline fast-symlink capacity or whose inline payload is not NUL-terminated exactly at i_size when the inode block is validated. This keeps malformed fast symlinks from reaching the read path. Validation reproduced this kernel report: KASAN use-after-free in ocfs2_fast_symlink_read_folio+0x12c/0x1f0 RIP: 0033:0x7f5c6d859aa7 Read of size 3905 Call trace: dump_stack_lvl+0x66/0xa0 (??) print_report+0xce/0x630 (??) ocfs2_fast_symlink_read_folio+0x12c/0x1f0 (fs/ocfs2/inode.c:?) srso_alias_return_thunk+0x5/0xfbef5 (??) __virt_addr_valid+0x19f/0x330 (??) kasan_report+0xe0/0x110 (??) kasan_check_range+0x105/0x1b0 (??) __asan_memcpy+0x23/0x60 (??) filemap_read_folio+0x27/0xe0 (??) filemap_read_folio+0x35/0xe0 (??) do_read_cache_folio+0x138/0x230 (??) __page_get_link+0x26/0x110 (??) page_get_link+0x2e/0x70 (??) vfs_readlink+0x15e/0x250 (??) touch_atime+0x4d/0x370 (??) do_readlinkat+0x186/0x200 (??) do_user_addr_fault+0x65a/0x890 (??) __x64_sys_readlink+0x46/0x60 (??) do_syscall_64+0x115/0x6a0 (arch/x86/entry/syscall_64.c:87) entry_SYSCALL_64_after_hwframe+0x77/0x7f (??)	2026-08-15	9.8	CVE-2026-74350
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvme: fix FDP fdpcidx bounds check The fdpcidx bounds check sets n = NUMFDPC + 1 but used > instead of >=, incorrectly accepting fdp_idx when it equals n (i.e. NUMFDPC + 1).	2026-08-15	9.8	CVE-2026-74361
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: md/raid10: reset read_slot when reusing r10bio for discard put_all_bios() always drops devs[i].bio, but it only drops devs[i].repl_bio when r10_bio->read_slot < 0. If discard reuses an r10bio that was previously used for a read, read_slot can still be non-negative, and discard cleanup can skip bio_put() on repl_bio. Reset read_slot to -1 when preparing an r10bio for discard so the replacement bio is always released correctly.	2026-08-15	9.8	CVE-2026-74376
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvme-multipath: fix flex array size in struct nvme_ns_head struct nvme_ns_head contains a flexible array member, current_path[], which is indexed using the NUMA node ID: head->current_path[numa_node_id()] The structure is currently allocated as: size = sizeof(struct nvme_ns_head) + (num_possible_nodes() * sizeof(struct nvme_ns *)); head = kzalloc(size, GFP_KERNEL); This allocation assumes that NUMA node IDs are sequential and densely packed from 0 .. num_possible_nodes() - 1. While this assumption holds on many systems, it is not always true on some architectures such as powerpc. On some powerpc systems, NUMA node IDs can be sparse. For	2026-08-15	9.8	CVE-2026-74384

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	example: NUMA: NUMA node(s): 6 NUMA node0 CPU(s): 80-159 NUMA node8 CPU(s): 0-79 NUMA node252 CPU(s): NUMA node253 CPU(s): NUMA node254 CPU(s): NUMA node255 CPU(s): That is, the possible/online NUMA node IDs are: 0, 8, 252, 253, 254, 255 In this case: num_possible_nodes() = 6 So memory is allocated for only 6 entries in current_path[]. However, the array is later indexed using the actual NUMA node ID. As a result, accesses such as: head->current_path[8] or head->current_path[252] goes out of bounds, leading to the following KASAN splat: <pre>===== BUG: KASAN: slab-out-of-bounds in nvme_mpath_revalidate_paths+0x22c/0x290 [nvme_core] Write of size 8 at addr c00020003bda35b8 by task kworker/u641:2/1997 CPU: 1 UID: 0 PID: 1997 Comm: kworker/u641:2 Not tainted 7.1.0-rc5-dirty #14 PREEMPT(lazy) Hardware name: 8335-GTH POWER9 0x4e1202 opal:siboot-v6.5.3-35-g1851b2a06 PowerNV Workqueue: async async_run_entry_fn Call Trace: [c000200037fa7510] [c00000000021c23d4] dump_stack_lvl+0x88/0xdc (unreliable) [c000200037fa7540] [c0000000009fda90] print_report+0x22c/0x67c [c000200037fa7630] [c0000000009fd508] kasan_report+0x108/0x220 [c000200037fa7740] [c0000000009fff48] __asan_store8+0xe8/0x120 [c000200037fa7760] [c008000018e76474] nvme_mpath_revalidate_paths+0x22c/0x290 [nvme_core] [c000200037fa7800] [c008000018e6556c] nvme_update_ns_info+0x4a4/0x5e0 [nvme_core] [c000200037fa7a50] [c008000018e66270] nvme_alloc_ns+0x6d8/0x1a70 [nvme_core] [c000200037fa7c20] [c008000018e679fc] nvme_scan_ns+0x3f4/0x630 [nvme_core] [c000200037fa7d10] [c00000000031f22c] async_run_entry_fn+0x9c/0x3a0 [c000200037fa7db0] [c0000000002fa544] process_one_work+0x414/0xa10 [c000200037fa7ec0] [c0000000002fbf00] worker_thread+0x320/0x640 [c000200037fa7f80] [c00000000030d0f8] kthread+0x278/0x290 [c000200037fa7fe0] [c00000000000ded8] start_kernel_thread+0x14/0x18 Allocated by task 1997 on cpu 1 at 35.928317s: The buggy address belongs to the object at c00020003bda3000 which belongs to the cache kmalloc-rnd-15-2k of size 2048 The buggy address is located 16 bytes to the right of allocated 1448-byte region [c00020003bda3000, c00020003bda35a8] The buggy address belongs to the physical page: Memory state around the buggy address: c00020003bda3480: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c00020003bda3500: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c00020003bda3580: 00 00 00 00 00 fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ^ c00020003bda3600: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc c00020003bda3680: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ===== Fix this by allocating the flexible array using nr_node_ids instead of num_possible_nodes(). Since nr_node_ids represents the maximum possible NUMA node IDs, indexing current_path[] using numa_node_id() becomes safe even on systems with sparse node IDs.</pre>			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/srpt: fix integer overflow in immediate data length check imm_buf->len is a user-controlled uint32_t received from the network. Adding it to imm_data_offset without overflow checking allows a malicious initiator to send len=0xFFFFFFFF, causing req_size to wrap around to a small value, bypassing the bounds check, and subsequently passing a ~4GB length to sg_init_one(). Use check_add_overflow() to detect wrapping before the comparison.	2026-08-15	9.8	CVE-2026-74394
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: addrconf: bail out of dad_failure when state is no longer POSTDAD addrconf_dad_failure() transitions ifp->state from DAD to POSTDAD via addrconf_dad_end(), which drops ifp->lock on return. The lock is re-acquired after net_info_ratelimited(). A concurrent ipv6_del_addr() can take the lock in that window, set ifp->state to DEAD and run list_del_rcu(&ifp->if_list). addrconf_dad_failure() then overwrites DEAD with ERDDAD at errdad: and schedules a new dad_work. The work calls ipv6_del_addr() again, hitting the already-poisoned list entry: general protection fault: 0000 [#1] SMP NOPTI CPU: 4 PID: 217 Comm: kworker/4:1 Workqueue: ipv6_addrconf addrconf_dad_work RIP: 0010:ipv6_del_addr+0xe9/0x280 RAX: dead000000000122 Call Trace: addrconf_dad_stop+0x113/0x140 addrconf_dad_work+0x28c/0x430 process_one_work+0x1eb/0x3b0 worker_thread+0x4d/0x400 kthread+0x104/0x140 ret_from_fork+0x35/0x40 Fold the addrconf_dad_end() logic into addrconf_dad_failure() under a single ifp->lock critical section. The STABLE PRIVACY branch temporarily drops ifp->lock around	2026-08-15	9.8	CVE-2026-74398

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	address regeneration, so at lock_errdad: verify the state is still POSTDAD before transitioning to ERRDAD; bail out otherwise to avoid overwriting a state set by another path while the lock was released.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dlm: fix add msg handle in send_queue ordered In a benchmark scenario triggering a lot of requests that triggers a lot of DLM messages on the network it can be that the mh->seq is not ordered according the oldest seq number. This ordering is required by dlm_receive_ack as "before(mh->seq, seq)" will stop to check for older sequence numbers that are ordered in the tail of "node->send_queue". The side effects of not having it correct ordered regarding "before(mh->seq, seq)" are refcounting issues and use-after free. I only was able to reproduce this issue in a experimental DLM branch and a user space DLM benchmark that uses io_uring. After changing this I don't experienced any refcounting with the sending buffer issues anymore.	2026-08-15	9.8	CVE-2026-74401
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: Fix potential null-ptr-deref in vxlan_gro_prepare_receive(). udp_tunnel_sock_release() could set sk->sk_user_data to NULL while vxlan_gro_prepare_receive() is running. Let's check if rcu_dereference_sk_user_data() is NULL after skb_gro_remchecksum_init().	2026-08-15	9.8	CVE-2026-74406
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: Fix netns teardown to cancel the preallocation charger Fix the teardown of an afs network namespace to make sure it cancels the work item that keeps the preallocated rxrpc call/conn/peer queue charged before incoming calls are disabled (i.e. listen 0). Also, if net->live is false because the afs netns is being deleted, make afs_charge_preallocation() skip charging and make afs_rx_new_call() avoid queueing the charger. (This was found by AI review).	2026-08-15	9.8	CVE-2026-74427
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix double unlock in rxrpc_recvmmsg() Fix a double unlock in rxrpc_recvmmsg() when dealing with OOB messages.	2026-08-15	9.8	CVE-2026-74428
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix UAF in rxgk_issue_challenge() Fix rxgk_issue_challenge() to free the page containing the challenge content after invoking the tracepoint as the whdr passed to the tracepoint points into the page just freed.	2026-08-15	9.8	CVE-2026-74433
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Don't move a peeked OOB message onto the pending queue rxrpc_recvmmsg_oob() takes a received oob message off recvmmsg_oobq and, if a response is needed, moves it onto the pending_oobq tree. However, only the unlink from recvmmsg_oobq is guarded by MSG_PEEK; the move onto pending_oobq always runs. As a result, reading a challenge with MSG_PEEK leaves the skb on recvmmsg_oobq while also adding it to pending_oobq. Since struct sk_buff's rbnode shares storage with its next and prev pointers, rb_insert_color() overwrites the list linkage, and the skb, which holds a single reference, becomes reachable from both queues at once. When the socket is closed both queues are drained in turn. While draining recvmmsg_oobq, __skb_unlink() follows the next and prev pointers that rbnode has overwritten and writes to a bad address. Also, as the skb holds a single reference but is freed from each queue, both the skb and the connection reference it holds are released twice. This leads to memory corruption and to a use-after-free caused by the connection refcount underflow. MSG_PEEK does not consume the message from the queue, so only unlink it from recvmmsg_oobq and then move it onto pending_oobq or free it when the message is actually consumed.	2026-08-15	9.8	CVE-2026-74434
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: serialize kernel accept preallocation with socket teardown rxrpc_kernel_charge_accept() reads rx->backlog without any socket/backlog synchronization and passes that raw pointer into rxrpc_service_prealloc_one(). A concurrent rxrpc_discard_prealloc() sets rx->backlog = NULL and frees the backlog rings, so a kernel preallocation worker can keep using a freed struct rxrpc_backlog while updating *_backlog_head/tail and array slots. Serialize the state check and backlog lookup with the socket lock, and reject kernel preallocation once teardown has disabled listening or discarded the service backlog.	2026-08-15	9.8	CVE-2026-74436
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Clear Present bit before tearing down scalable-mode context entry device_pasid_table_teardown() zeroes the 128-bit scalable-mode context entry with context_clear_entry() while the Present bit is still set. This creates a window where the hardware can fetch a torn entry, with some fields already zeroed while Present is still set, leading to unpredictable behavior or spurious faults. The	2026-08-15	9.3	CVE-2026-74439

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	context-cache invalidation is issued only after the entry has been zeroed, and intel_pasid_free_table() then frees the PASID directory pages, so the IOMMU can keep walking a stale Present=1 entry that points at freed memory. While x86 provides strong write ordering, the compiler may reorder the two 64-bit writes to the entry, and the hardware fetch is not guaranteed to be atomic with respect to multiple CPU writes. Commit c1e4f1dccbe9d ("iommu/vt-d: Clear Present bit before tearing down context entry") fixed this exact pattern in domain_context_clear_one() and the copied-context path, but device_pasid_table_takedown() was not converted. Align it with the "Guidance to Software for Invalidations" in the VT-d spec, Section 6.5.3.3, using the same ownership handshake as the sibling fix: clear only the Present bit, flush it to the IOMMU, perform the context-cache invalidation, and only then zero the rest of the entry.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: use pskb_network_may_pull() in route_shortcircuit() route_shortcircuit() currently calls pskb_may_pull(skb, sizeof(struct iphdr)) (or ipv6hdr), which checks if bytes are available starting from skb->data. However, in vxlan_xmit(), skb->data points to the MAC header, so skb_network_offset(skb) is ETH_HLEN (14 bytes). Using pskb_may_pull(skb, 20) only checks 20 bytes from skb->data (which is 14 bytes MAC header + 6 bytes of IP header), leaving the rest of the IP header potentially un-pulled in non-linear frags. Subsequent dereferences of ip_hdr(skb)->daddr can read beyond the pulled linear buffer length. Fix this by using pskb_network_may_pull(), which adds skb_network_offset(skb) to the length check to ensure the full network header is present in the linear buffer.	2026-08-15	9.8	CVE-2026-74473
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: use pskb_network_may_pull() for transmit path header pulls In vxlan_xmit(), arp_reduce(), and vxlan_mdb_entry_skb_get(), pskb_may_pull() was being called to verify the availability of network layer headers (ARP, IPv6/ND, IP/IPv6 MDB keys). However, during transmit skb->data points to the MAC header, so skb_network_offset(skb) is ETH_HLEN (14 bytes). Using pskb_may_pull(skb, len) only checks len bytes from skb->data rather than skb_network_offset(skb) + len, which can leave part of the network header in non-linear frags. Replace these remaining pskb_may_pull() calls with pskb_network_may_pull() to properly account for the MAC header offset.	2026-08-15	9.8	CVE-2026-74474
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: veth: convert frag_list skbs before running XDP A frag_list skb can reach veth with data_len set but nr_frags zero. veth_convert_skb_to_xdp_buff() only converts skbs that are shared, locked, have frags[], or do not have enough headroom. It later uses skb_is_nonlinear() to decide whether to set XDP_FLAGS_HAS_FRAGS and xdp_frags_size. That exposes frag_list data to XDP as if it were stored in frags[], but frags[] is empty. AF_XDP copy mode can then trust the bogus XDP fragment metadata, walk an empty fragment entry, and crash in memcpy() from __xsk_rcv(). Route non-linear skbs through skb_pp_cow_data() before exposing them to XDP, and only advertise XDP frags when the resulting skb has frags[]. skb_copy_bits() already handles frag_list input, and skb_pp_cow_data() builds frags[] output with skb_add_rx_frag(), which is the representation XDP multi-buffer expects.	2026-08-15	9.1	CVE-2026-74476
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: um: vector: fix use-after-free in vector_mmsg_rx() When vector_mmsg_rx() discards a packet whose overlay header fails verify_header(), it frees the skb and continues the loop: if (header_check < 0) { dev_kfree_skb_irq(skb); vp->estats.rx_encaps_errors++; continue; } The normal and short-packet paths fall through to the bottom of the loop body, which clears the consumed slot and advances the cursors: (*skbuff_vector) = NULL; mmsg_vector++; skbuff_vector++; The verify_header() < 0 path skips that via continue, so the freed skb is left in skbuff_vector[] and the cursors do not advance. The next iteration reads the same slot, gets the freed skb, and frees it again, producing a refcount underflow / use-after-free in the RX path. Discard the slot the same way the other paths do before continuing. Only transports whose verify_header() can return negative are affected: GRE and L2TPv3 do so on a cookie/session-id mismatch (raw/tap do not), so any peer on such a transport can trigger it without authentication.	2026-08-15	9.8	CVE-2026-74478
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: bridge: stop fast-leave after deleting a port group br_multicast_leave_group() iterates mp->ports with pp = &p->next in its fast-leave path. After br_multicast_del_pg() removes p, continuing the loop advances pp through the deleted entry. If multicast-to-unicast was enabled, the bridge can hold multiple port groups for the	2026-08-15	9.8	CVE-2026-74480

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	same port and group with different source MAC addresses. Once multicast-to-unicast is disabled, br_port_group_equal() matches those entries by port only. A fast leave can then delete one entry and continue from its stale next pointer, leaving mp->ports pointing at a deleted port group. Fast leave only needs to remove one matching port group. Break after br_multicast_del_pg() so the loop stops before dereferencing the removed entry.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix socket use-after-free during link group termination __smc_lgr_terminate() drops conns_lock after finding a connection in lgr->conns_all, but before taking a reference on its socket. The connection is embedded in the socket, and its registration reference protects it only while the connection remains in the tree. A concurrent close can unregister the connection and drop that reference, freeing the socket before the termination worker reaches sock_hold(). The race is reachable when close overlaps link group termination. Local stress testing reproduced the use-after-free and KASAN reported: BUG: KASAN: slab-use-after-free in __smc_lgr_terminate.part.0 [smc] Write of size 4 by task kworker/3:3 Workqueue: events smc_lgr_terminate_work [smc] __smc_lgr_terminate.part.0 [smc] The socket was allocated by smc_create(), freed through slab_free_after_rcu_debug(), and was followed by: refcount_t: addition on 0; use-after-free. __smc_lgr_terminate.part.0 [smc] Take the socket reference while conns_lock still protects the tree entry. The unregister path then cannot drop the last reference until termination has finished using the socket.	2026-08-15	9.8	CVE-2026-74493
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: igbvf: Fix leak in TX DMA error cleanup If an error is encountered while mapping TX buffers, the driver should unmap any buffers already mapped for that skb. Because count is incremented before each frag mapping, it will always match the correct number of unmappings needed when dma_error is reached. Decrementing count before the while loop in dma_error causes an off-by-one error. If any mapping was successful before an unsuccessful mapping, exactly one DMA mapping (the head) would leak. This bug was introduced by a 2010 fix for an endless loop in dma_error. All other affected drivers have already been fixed.	2026-08-15	9.8	CVE-2026-74495
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Cancel delayed I/O APIC EOI handling before destroying vCPUs Cancel (and flush) the I/O APIC's delayed EOI handling work during the "pre VM destroy" phase, before vCPUs are destroyed, as processing the EOI broadcast will inject another IRQ if the line is asserted, i.e. will try to deliver an IRQ to the target vCPU(s). Canceling the work after vCPUs are destroyed leads to UAF if the delayed work is processed after vCPUs are destroyed. BUG: KASAN: slab-use-after-free in __kvm_irq_delivery_to_apic_fast+0x9bf/0xa20 arch/x86/kvm/lapic.c:1250 Read of size 8 at addr ffff8880499abea0 by task kworker/1:2/1218 CPU: 1 UID: 0 PID: 1218 Comm: kworker/1:2 Not tainted 7.1.0-rc7 #5 PREEMPT(lazy) Hardware name: QEMU Ubuntu 25.10 PC v2 (i440FX + PIIX, + 10.1 machine, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Workqueue: events kvm_ioapic_eoi_inject_work Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 dump_stack_lvl+0x100/0x190 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 print_report+0x139/0x4ad mm/kasan/report.c:482 kasan_report+0xe4/0x1d0 mm/kasan/report.c:595 __kvm_irq_delivery_to_apic_fast+0x9bf/0xa20 arch/x86/kvm/lapic.c:1250 __kvm_irq_delivery_to_apic+0xd8/0xbf0 arch/x86/kvm/lapic.c:1345 kvm_irq_delivery_to_apic arch/x86/kvm/lapic.h:129 ioapic_service+0x308/0x590 arch/x86/kvm/ioapic.c:492 kvm_ioapic_eoi_inject_work+0x13c/0x190 arch/x86/kvm/ioapic.c:532 process_one_work+0xa59/0x19a0 kernel/workqueue.c:3314 process_scheduled_works kernel/workqueue.c:3397 worker_thread+0x5eb/0xe50 kernel/workqueue.c:3478 kthread+0x370/0x450 kernel/kthread.c:436 ret_from_fork+0x72b/0xd30 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK> Note, the VM is unreachable once kvm_destroy_vm() starts, and scheduling new work via kvm_ioapic_send_eoi() can only be done via KVM_RUN, i.e. requires a live vCPU. Alternatively, KVM could simply destroy the I/O APIC during the "pre" phase of VM destruction, but that gets more than a bit sketchy as KVM expects the I/O APIC to exist if ioapic_in_kernel() is true, and nested virtualization in particular has a bad habit of touching VM-scope state during vCPU destruction. E.g. attempting to free the PIC during the pre phase would lead to a NULL pointer dereference in kvm_cpu_has_extint(), and it's not hard to imagine the I/O APIC having a similar flaw.	2026-08-15	9.3	CVE-2026-74517

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: use memcmp() to compare ClientGUIDs ClientGUID is a fixed-size binary value and can contain embedded NUL bytes. strncmp() stops comparing at the first NUL byte, so different ClientGUID values can incorrectly be treated as equal. Use memcmp() in SMB3 multichannel session binding and FSCTL_VALIDATE_NEGOTIATE_INFO to compare all SMB2_CLIENT_GUID_SIZE bytes.	2026-08-15	9.1	CVE-2026-74521
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rtase: fix double free of multi-frag skb on DMA map failure In rtase_start_xmit(), when the head buffer DMA mapping fails after rtase_xmit_frags() has mapped all fragments, the error path clears the fragment descriptors with rtase_tx_clear_range(), which frees the skb through the last-frag slot and accounts tx_dropped. Control then falls through to the common error label, which frees the same skb a second time and counts it again. Return right after clearing the fragments when the skb owns frags; the no-frag case still drops through and frees the head skb once.	2026-08-15	9.8	CVE-2026-74545
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: libiscsi_tcp: Bound SCSI Response data segment to the connection buffer iscsi_tcp_hdr_dissect() receives the data segment of several PDU types into the fixed-size conn->data buffer, which is allocated for ISCSI_DEF_MAX_RECV_SEG_LEN (8192) bytes. For the LOGIN_RSP, TEXT_RSP, REJECT and ASYNC_EVENT opcodes the dissect path already rejects a PDU whose DataSegmentLength exceeds that buffer. The SCSI Command Response (ISCSI_OP_SCSI_CMD_RSP) path also copies its data segment (sense/response data) into conn->data via iscsi_tcp_data_rcv_prep(), but it does so without the same check. The only upstream bound on in.dataalen is conn->max_rcv_dlength, the initiator's advertised MaxRecvDataSegmentLength, which is commonly negotiated well above 8192 (open-iscsi defaults to 262144). A target that returns a SCSI Response with a DataSegmentLength between 8193 and max_rcv_dlength therefore overflows the 8192-byte conn->data buffer. Once the same bound applies, ISCSI_OP_SCSI_CMD_RSP is handled exactly like those responses: bound the data segment, receive it into conn->data when present, and otherwise complete the PDU with no data. Fold the opcode into that case group rather than duplicating the check.	2026-08-15	9.8	CVE-2026-74556
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic: Fix race between LPI release and re-registration Fix a potential race between decrementing an LPI's reference count and evicting that structure from the LPI xarray. LPI structures are maintained in the VGIC LPI xarray (dist->lpi_xa). When the reference count of an LPI structure drops to zero, vgic_release_lpi_locked() removes the structure from the xarray and frees it under the xarray lock. However, the release of an LPI can race with a concurrent LPI re-registration with the same INTID via vgic_add_lpi() on another CPU, since the reference count drop and the xarray eviction are not performed in a single atomic step. This can happen e.g. if the guest issues a DISCARD while the LPI is still referenced from a vCPU's active-pending list (ap_list), and the same INTID is re-mapped via MAPTI. Particularly, vgic_release_lpi_locked() is called from two distinct paths: direct release via vgic_put_irq(), and deferred release via vgic_release_deleted_lpis(). During direct release, the issue can result in deleting a newly registered LPI from the xarray: CPU0 (Releasing LPI) CPU1 (Adding new LPI) ===== ===== vgic_put_irq() __vgic_put_irq() refcount_dec_and_test() vgic_add_lpi() xa_lock_irqsave() old_irq = xa_load(.., intid) vgic_try_get_irq_ref(old_irq) == false new IRQ inserted --> __xa_store(.., intid, ..) xa_unlock_irqrestore() xa_lock_irqsave(); vgic_release_lpi_locked() __xa_erase(.., irq->intid) <-- BUG: new IRQ is erased kfree_rcu(old_irq) During the deferred release path, the old IRQ can be leaked: CPU0 (Releasing LPI) CPU1 (Adding new LPI) ===== ===== vgic_put_irq_norelease() __vgic_put_irq() refcount_dec_and_test() irq->pending_release = true vgic_add_lpi() xa_lock_irqsave() old_irq = xa_load(.., intid) vgic_try_get_irq_ref(oldirq) == false BUG: old IRQ overwritten --> __xa_store(.., intid, ..) xa_unlock_irqrestore() vgic_release_deleted_lpis() xa_lock_irqsave() xa_for_each() { .. } <-- old IRQ with pending_release = true is gone, so it cannot be released To fix the direct release path, move the reference count drop inside the xarray lock, making sure that vgic_add_lpi() never encounters the to-be-released LPI. In the deferred release path, the refcount drop must happen under a raw spinlock, so the xarray lock cannot be grabbed, and the same solution does not work. Instead, update vgic_add_lpi(), so that if it evicts an LPI from the xarray, it takes on the responsibility of freeing it. Consequently, an LPI may now be freed	2026-08-15	9.3	CVE-2026-74568

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	concurrently after a deferred release drops the refcount, so accessing the pending_release field is no longer safe from use-after-free. Delete all uses of the flag, and update vgic_release_deleted_lpis() to identify orphaned LPIs purely based on their refcount.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_sip: widen NAT rewrite delta to s32 in sip_help_tcp() sip_help_tcp() stores the size change of each NAT-rewritten SIP message in s16 diff and accumulates it in s16 tdiff, but a single message can grow by more than S16_MAX while the packet stays under the 65535 enlarge_skb() limit: nf_nat_sip() rewrites every matching URI, and a long Contact list expands the message by tens of kilobytes. diff then wraps, and "datalen = datalen + diff - msglen" yields a huge unsigned datalen, so the next iteration's ct_sip_get_header() reads past the linearized skb tail. Widen diff, tdiff and the seq_adjust hook to s32. Both are bounded by the 65535 byte packet limit, and the seqadj core is already s32 (nf_ct_seqadj_set() takes s32), so no previously accepted input is rejected. BUG: KASAN: use-after-free in ct_sip_get_header (net/netfilter/nf_conntrack_sip.c:464) Read of size 1 at addr ffff888010800000 by task ksoftirqd/1/25 ct_sip_get_header (net/netfilter/nf_conntrack_sip.c:464) sip_help_tcp (net/netfilter/nf_conntrack_sip.c:1694) nf_confirm (net/netfilter/nf_conntrack_proto.c:183) nf_hook_slow (net/netfilter/core.c:619) ip6_output (net/ipv6/ip6_output.c:246) ip6_forward (net/ipv6/ip6_output.c:690) ipv6_rcv (net/ipv6/ip6_input.c:351) __netif_receive_skb_one_core (net/core/dev.c:6212) process_backlog (net/core/dev.c:6676) __napi_poll (net/core/dev.c:7735) net_rx_action (net/core/dev.c:7955) handle_softirqs (kernel/softirq.c:622) run_ksoftirqd (kernel/softirq.c:1076) ...	2026-08-15	9.8	CVE-2026-74569
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: harden runlist realloc size calculations Add a shared helper to safely convert runlist element counts to byte sizes using overflow checks, and use it in both ntfs_rl_realloc() and ntfs_rl_realloc_nofail().	2026-08-15	9.8	CVE-2026-74570
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu-v3-iommufd: Require exactly one Stream ID for a vDEVICE arm_vsmmu_vsid_to_sid() maps a guest's vSID to a single physical Stream ID taken from master->streams[0], assuming a device has exactly one stream. A device with several streams gets only its first one mapped, so a guest vSID invalidation cannot reach the others' ATC and IOTLB entries; a device with none makes master->streams a ZERO_SIZE_PTR, read out of bounds. Add an arm_vsmmu_vdevice_init() op to reject the vDEVICE with -EOPNOTSUPP when master->num_streams is not one, rather than mapping it silently.	2026-08-15	9.3	CVE-2026-74573
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_uart: clear HCI_UART_SENDING when write_work is canceled HCI_UART_SENDING bit in tx_state means write_work is pending and blocks queueing it again. Currently this bit is not cleared when canceling the work in hci_uart_close(), which blocks future writes when device is reopened later if write_work was pending. Fix by clearing HCI_UART_SENDING when canceling the work. Also make clearing of tx_skb safe by using disable_work_sync + enable_work instead of just cancel_work_sync. hci_uart_flush() purges the proto tx queue so we can cancel the pending write_work there, instead of doing it just in hci_uart_close(). Re-enable and possibly requeue the work after queue flush.	2026-08-10	8	CVE-2026-68085
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: HID: wacom: stop hardware after post-start probe failures wacom_parse_and_register() starts HID hardware before registering inputs and initializing pad LEDs/remotes. Those later steps can fail, but their error paths currently release Wacom resources without stopping the HID hardware. Route post-hid_hw_start() failures through hid_hw_stop() before releasing driver resources. This issue was identified during our ongoing static-analysis research while reviewing kernel code.	2026-08-10	8.8	CVE-2026-68091
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate ACE size against SID sub-authorities set_ntacl_dacl() validates sid.num_subauth before copying an ACE, but does not verify that the declared ACE size contains all sub-authorities described by that field. An undersized ACE can therefore be copied and later make the POSIX ACL deduplication walk inspect data beyond the copied ACE boundary. The existing initial bound check is also too small. It only ensures that the ACE size field is accessible before set_ntacl_dacl() reads sid.num_subauth farther into the input buffer. Require enough input for the fixed SID header before accessing num_subauth, reject ACEs smaller than that header, and skip ACEs	2026-08-10	8.8	CVE-2026-68097

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	whose declared size cannot contain the complete SID. This makes the validation consistent with the other ACE walk paths.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: bound DACL dedup walk to copied ACEs set_ntacl_dacl() can stop copying ACEs before consuming the full input DACL when size accounting overflows. When that happens, num_aces reflects only the ACEs that were actually copied into the output DACL, but set_posix_acl_entries_dacl() still receives nt_num_aces and uses it to walk the existing ACE array during dedup. That makes the dedup walk scan past the copied ACE array and inspect buffer tail that does not contain valid ACEs. Split the two meanings currently carried by the NT ACE count. Pass the number of copied NT ACEs to bound the dedup walk, and preserve the original "input DACL had NT ACEs" state separately for the Everyone/default ACL fallback. This keeps the dedup walk aligned with the ACEs that are actually present in the rebuilt DACL.	2026-08-10	8.8	CVE-2026-68098
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate num_subauth when copying ACE in set_ntacl_dacl set_ntacl_dacl() copies each ACE from the attacker-controlled stored security descriptor verbatim into the response DACL without checking sid.num_subauth. The ACE bytes (including an unchecked num_subauth) originate from an authenticated SMB2_SET_INFO(SecInfo=DACL) that is stored raw via ksmbd_vfs_set_sd_xattr(); parse_dacl() rejects a bad ACE with 'break' rather than an error, so parse_sec_desc() still returns success and the malformed SD reaches the xattr intact. On a subsequent SMB2_QUERY_INFO(SecInfo=DACL) for an inode carrying a POSIX access ACL, build_sec_desc() -> set_ntacl_dacl() -> set_posix_acl_entries_dacl() walks the copied ACEs and reads ntace->sid.sub_auth[ntace->sid.num_subauth - 1] with num_subauth taken straight from the stored SD. Since sub_auth[] is fixed at SID_MAX_SUB_AUTHORITIES (15), a crafted num_subauth (e.g. 255) drives an out-of-bounds heap read of ~1 KB with an offset fully controlled by an authenticated client. The sibling functions already gate this field: parse_dacl() -- num_subauth == 0 > SID_MAX_SUB_AUTHORITIES parse_sid() -- num_subauth > SID_MAX_SUB_AUTHORITIES smb_copy_sid() -- min_t(u8, num_subauth, SID_MAX_SUB_AUTHORITIES) set_ntacl_dacl() is the lone inconsistent path that omits the check. Add the same num_subauth validation in set_ntacl_dacl() before copying the ACE, matching the gate already enforced by parse_dacl().	2026-08-10	8.1	CVE-2026-68100
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vcn4: avoid rereading IB param length Reuse the parameter length returned by vcn_v4_0_enc_find_ib_param() instead of rereading it from the IB. This avoids a potential TOCTOU issue if the IB contents change between reads. (cherry picked from commit dbb02b4755f8c1f3773263f2d779872c1c0c073a)	2026-08-10	8.8	CVE-2026-68107
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vce: fix integer overflow in image size Fix a security vulnerability where malicious VCE command streams with oversized dimensions (e.g. 65536--65536) cause 32-bit integer overflow, wrapping the calculated buffer size to 0. This bypasses validation and allows GPU firmware to perform out-of-bound memory access. The fix uses 64-bit arithmetic to detect overflow and rejects invalid dimensions before they reach the hardware. V2: remove redundant check V3: modify max height value V4: remove size64 (cherry picked from commit cbe408dba581755ad1279a487ec786d8927d778d)	2026-08-10	8.8	CVE-2026-68108
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: challenge ACK for non-exact RST in SYN-RECEIVED The SYN-RECEIVED request-socket path in tcp_check_req() accepts an in-window RST without requiring SEG.SEQ to exactly match RCV.NXT. A non-exact RST therefore removes the request instead of eliciting a challenge ACK. RFC 9293 section 3.10.7.4 applies the RFC 5961 reset check in SYN-RECEIVED: an exact RST resets the connection, while a non-exact in-window RST must trigger a challenge ACK and be dropped. Apply that check before the ACK-field validation, following the RFC sequence-number, RST, then ACK processing order. Factor the per-netns challenge ACK quota out of tcp_send_challenge_ack() so request sockets can share it. Use the request socket's send_ack() callback and its own out-of-window ACK timestamp to send and rate-limit the response.	2026-08-10	8.2	CVE-2026-68118
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mac802154: llsec: reject frames shorter than the authentication tag llsec_do_decrypt_auth() computes the associated-data length for the AEAD request as assoclen += datalen - authlen; where datalen is the number of bytes after the MAC header and authlen (4, 8 or 16) is the length of the authentication tag. Nothing verifies that the frame	2026-08-10	8.8	CVE-2026-68125

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	actually carries at least authlen payload bytes. A secured frame whose payload is shorter than the tag makes datalen - authlen negative; assoclen is then passed to aead_request_set_ad() as an unsigned value close to 4 GiB, so crypto_aead_decrypt() walks far off the end of the scatterlist that only spans the real frame. The frame is fully attacker-controlled and reaches this path from any IEEE 802.15.4 peer in radio range. Reject frames whose payload is shorter than the authentication tag before the subtraction. Dynamically reproduced on a KASAN kernel as a general-protection-fault in the AEAD scatterwalk, and the fix confirmed.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ice: reject out-of-range ptype in ice_parser_profile_init set_bit(rslt->ptype, prof->ptypes) operates on a DECLARE_BITMAP of ICE_FLOW_PTYPE_MAX (1024) bits. Nothing prevents a malicious VF from providing ptype >= 1024 through VIRTCHNL, resulting in a write past the end of the bitmap and a kernel page fault. Reproduced with a custom kernel module injecting a crafted VIRTCHNL_OP_ADD_RSS_CFG on E810-C QSFP (8086:1592), FW 4.91 0x800214af 1.3909.0, ICE COMMS DDP 1.3.53.0, kernel 7.1.0-rc1. crash_parser: ice_parser_profile_init @ ffffffff0d61b60 crash_parser: setting ptype=0xffff (max valid=1023) crash_parser: calling ice_parser_profile_init - expect OOB crash! BUG: kernel NULL pointer dereference, address: 0000000000000000 Oops: Oops: 0002 [#1] SMP NOPTI CPU: 56 UID: 0 PID: 165011 Comm: insmod Kdump: loaded Tainted: G S U OE 7.1.0-rc1 #1 Hardware name: Intel Corporation S2600BPB/S2600BPB RIP: 0010:ice_parser_profile_init+0x2d/0x1d0 [ice] Call Trace: <TASK> ? __pfx_ice_parser_profile_init+0x10/0x10 [ice] crash_init+0x127/0xff0 [crash_parser] do_one_initcall+0x45/0x310 do_init_module+0x64/0x270 init_module_from_file+0xcc/0xf0 idempotent_init_module+0x17b/0x280 __x64_sys_finit_module+0x6e/0xe0 Bail out early with -EINVAL when ptype is out of range.	2026-08-10	8.8	CVE-2026-68128
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use-after-free of a severed iucv_path af_iucv queues not-yet-received message notifications on iucv->message_q, each holding a raw pointer to the connection's iucv_path. When the peer severs the connection, iucv_sever_path() frees that path with iucv_path_free() but leaves the notifications queued. A later recvmmsg() drains message_q via iucv_process_message_q() and hands the stale path to message_receive() -- a use-after-free of the freed iucv_path. Drop the queued notifications when the path is severed; once the path is gone they can no longer be received. This also frees the notifications leaked when a socket is closed with messages still queued.	2026-08-10	8.8	CVE-2026-68140
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: geneve: require CAP_NET_ADMIN in the device netns for changelink A tunnel changelink() operates on at most two netns, dev_net(dev) and the sticky underlay netns geneve->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in geneve->net can rewrite a geneve device whose underlay lives in geneve->net. geneve_changelink() applies the new configuration against geneve->net: geneve_link_config() and the geneve_quiesce()/geneve_unquiesce() pair reopen the underlay sockets in that netns (geneve_sock_add() uses geneve->net), so the same reasoning as the tunnel changelink series applies here. Gate geneve_changelink() with rtnl_dev_link_net_capable(), at the top of the op before any attribute is parsed, matching ipgre_changelink() and the rest of the "require CAP_NET_ADMIN in the device netns for changelink" series. Found by Osec automated security-research tooling (https://Osec.ai).	2026-08-10	8.8	CVE-2026-68142
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs: preserve ACL_DONT_CACHE state in forget_cached_acl() The ACL_DONT_CACHE state is meant to be a constant state for the inode for filesystems that want to opt out of posix acl caching. Commit facd61053cff1 ("fuse: fixes after adapting to new posix acl api") used this facility to opt out of posix acl caching for fuse inodes with fuse server that does not negotiate FUSE_POSIX_ACL (fc->posix_acl). The commit also takes care to gate the forget_all_cached_acls() call in fuse_set_acl() on fc->posix_acl because there is no need for it, but there are other placed in fuse code which call forget_all_cached_acls() unconditional to fc->posix_acl and those cause the loss of the ACL_DONT_CACHE state. This is not only a functional bug. Properly timed, a get_acl() from this fuse filesystem can return a stale cached value, as was observed in tests, because set_acl() does not invalidate the unintentional acl cache. We could fix this in fuse, but it actually makes no sense for the vfs helper	2026-08-10	8.4	CVE-2026-68149

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	forget_cached_acl() to invalidate the ACL_DONT_CACHE state, so let it not do that to fix fuse and future users of ACL_DONT_CACHE.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: misc: nsm: only unlock nsm_dev on post-lock error paths nsm_dev_ioctl() jumps to the common out label even when the initial copy_from_user() fails before nsm->lock has been taken. The error path then blindly unlocks a mutex that was never acquired. This issue was found by our static analysis tool and then manually reviewed against the current tree. The grounded PoC kept the miscdevice ioctl entry and the pre-lock copy_from_user(&raw, argp, _IOC_SIZE(cmd)) failure path by issuing NSM_IOCTL_RAW with an invalid user pointer. That failure reaches the shared out label before mutex_lock(&nsm->lock). Lockdep reported: WARNING: bad unlock balance detected! exploit/193 is trying to release lock (&global_nsm.lock) at: nsm_dev_ioctl+0x5f/0xcf [vuln_msv] but there are no more locks to release! no locks held by exploit/193. Return immediately on the pre-lock copy_from_user() failure and keep the common unlock label for the post-lock paths only.	2026-08-10	8.4	CVE-2026-68179
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: make release_scratchbuffers idempotent brcmf_pcie_release_scratchbuffers() frees the shared.scratch and shared.ringupd DMA buffers with dma_free_coherent() but does not clear the pointers afterwards, unlike the sibling release_ringbuffers() which NULLs commonrings/flowrings/idxbuf on release. Both the bus_reset .reset callback (brcmf_pcie_reset) and brcmf_pcie_remove() call release_scratchbuffers. When reset teardown has run before removal, remove's own teardown would call dma_free_coherent() a second time on the already-freed DMA allocation. NULL the pointers after free, matching release_ringbuffers(), so a later release observes that the allocation has already been released. This patch makes repeated sequential release safe; the reset-work lifetime is handled separately by the following patch. This issue was found by an in-house static analysis tool.	2026-08-10	8.8	CVE-2026-68192
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: wilc1000: validate assoc response length before subtracting header wilc_parse_assoc_resp_info() computes the trailing IE length as ies_len = buffer_len - sizeof(*res); without first checking that buffer_len is at least sizeof(struct wilc_assoc_resp) (6 bytes). buffer_len is the length reported for a received association response (host_int_parse_assoc_resp_info() passes hif_drv->assoc_resp / assoc_resp_info_len straight in) and must be validated before the driver accesses the fixed header. For a frame shorter than the 6-byte fixed header, the subtraction wraps. For a four-byte response the result is truncated to a u16 ies_len of 65534, so kmemdup() then attempts to copy 65534 bytes starting at buffer + sizeof(*res), beyond the valid association-response data (CWE-125). A response shorter than four bytes can also cause an out-of-bounds read of res->status_code at offsets 2 and 3. Reject frames too short to hold the fixed header before touching the header or computing ies_len. Also set the connection status to a failure on this path: the caller falls through to a "conn_info->status == WLAN_STATUS_SUCCESS" check after the parser returns, so leaving the status untouched could let a malformed short response be treated as a successful association.	2026-08-10	8.3	CVE-2026-68196
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath6kl: fix use-after-free in aggr_reset_state() The aggr_reset_state() function uses timer_delete() (non-synchronous) for the aggregation timer before proceeding to delete TID state and before the structure is freed by callers like aggr_module_destroy(). If the timer callback (aggr_timeout) is executing when aggr_reset_state() is called, the callback will continue to access aggr_conn fields like rx_tid[] and stat[] which may be freed immediately after by kfree(aggr_info->aggr_conn) in aggr_module_destroy(). Additionally, the timer callback can re-arm itself via mod_timer() while aggr_reset_state() is running, creating a more complex race condition. Use timer_delete_sync() instead to ensure any running timer callback has completed before returning.	2026-08-10	8.8	CVE-2026-68198
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath6kl: fix OOB access from firmware ADDBA window size aggr_rcv_addba_req_evt() logs a debug message when the firmware-supplied win_sz is outside [AGGR_WIN_SZ_MIN, AGGR_WIN_SZ_MAX] but does not return. The out-of-range win_sz is then used in TID_WINDOW_SZ() to compute a kcalloc size and stored in rxtid->hold_q_sz, leading to zero-size or overflowed allocations and subsequent out-of-bounds access. Clean up any previously active aggregation session for the	2026-08-10	8.8	CVE-2026-68199

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	TID first, then return early when win_sz is out of the valid range, instead of proceeding with a broken allocation size.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/gpusvm: publish dpagemap early to avoid device mapping leak on error drm_gpusvm_get_pages() only stored the local dpagemap into svm_pages->dpagemap on the success path. If a later page failed (e.g. -EOPNOTSUPP when ctx->allow_mixed is false) and jumped to err_unmap, svm_pages->dpagemap was still NULL, so __drm_gpusvm_unmap_pages() skipped device_unmap() and leaked the device mappings already created. Assign svm_pages->dpagemap when the first device page is mapped so the err_unmap path can device_unmap() those mappings. This issue was found by Sashiko AI review.	2026-08-10	8.8	CVE-2026-68240
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tracing: Fix use-after-free freeing trigger private data Commit 61d445af0a7c ("tracing: Add bulk garbage collection of freeing event_trigger_data") moved the kfree() of event_trigger_data to a kthread that runs tracepoint_synchronize_unregister() before freeing. That removed the synchronization the trigger.free callbacks used to get implicitly and inline from trigger_data_free(). event_hist_trigger_free(), event_hist_trigger_named_free() and event_enable_trigger_free() free their satellite data (hist_data, cmd_ops, enable_data) right after trigger_data_free() returns. With the synchronization now deferred to the kthread, a concurrent tracepoint handler can still reach that data through the list_del_rcu()'d trigger, causing a use-after-free. The histogram teardown must stay synchronous: remove_hist_vars() and unregister_field_var_hists() have to detach a synthetic event from the histogram before the trigger-removal write returns, otherwise a following command races in and the synthetic-event removal fails with -EBUSY, as the trigger-synthetic-eprobe.tc selftest catches. Make those callbacks wait with the correct barrier - tracepoint_synchronize_unregister(), matching the free kthread - before freeing. The enable trigger has no such synchronous requirement, and a blocking synchronize there would re-serialize the path that commit deliberately deferred. Give it an optional private_data_free() callback that the free kthread runs after its grace period, and free enable_data from there.	2026-08-10	8.8	CVE-2026-68283
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: restrict socket creation to the initial network namespace QRTR keeps its entire port and node state in module-global variables that are not partitioned per network namespace: qrtr_local_nid is a single global node id (always 1) and qrtr_ports is a single global xarray. qrtr_port_lookup() and qrtr_local_enqueue() operate on that global state with no network-namespace check, and qrtr_create() places no restriction on the namespace a socket is created in. As a result an unprivileged process that creates an AF_QIPCRTR socket in a separate network namespace, e.g. via unshare(CLONE_NEWUSER CLONE_NEWNET), can send QRTR datagrams - including control-plane messages such as QRTR_TYPE_NEW_SERVER - to QRTR sockets owned by another namespace, and vice versa. The receiving socket sees such a message as coming from node id 1, indistinguishable from a legitimate local client, breaking the isolation that network namespaces are expected to provide. QRTR is a transport to global hardware endpoints (the modem and other remote processors) and has no per-namespace semantics; its in-kernel name service already creates its socket in init_net only. Confine the socket family to the initial network namespace, as other non-namespace-aware socket families do (see llc_ui_create() and the ieee802154 socket code).	2026-08-10	8.8	CVE-2026-68294
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: bound uAP association event IEs to the event buffer mwifiex_process_uap_event() handles EVENT_UAP_STA_ASSOC by exposing the (re)association request IEs that the firmware copies into the event: sinfo->assoc_req_ies = &event->data[len]; len = (u8 *)sinfo->assoc_req_ies - (u8 *)&event->frame_control; sinfo->assoc_req_ies_len = le16_to_cpu(event->len) - (u16)len; event->len is supplied by the device firmware and is never validated, and the subtraction is unchecked. assoc_req_ies points into adapter->event_body[MAX_EVENT_SIZE], a fixed-size array embedded in the kmalloc()'d struct mwifiex_adapter. On the ap_11n_enabled path mwifiex_set_sta_ht_cap() walks these IEs with cfg80211_find_ie(), whose for_each_element() loop dereferences each element header. A firmware-reported event->len larger than the bytes actually received makes assoc_req_ies_len describe IEs that extend past event_body, so the walk reads out of the adapter slab object, a slab-out-of-bounds read (KASAN: slab-out-of-bounds in cfg80211_find_ie). An event->len smaller than the header instead makes the int subtraction negative, which wraps to a huge size_t when stored in	2026-08-10	8.8	CVE-2026-68326

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	assoc_req_ies_len. The same length is handed to cfg80211_new_sta(), so a more modest over-claim can also copy stale event_body bytes into the NL80211_CMD_NEW_STATION notification. A malicious or malfunctioning mwifiex device (USB/SDIO/PCIe) can deliver such an event while the interface is in AP/uAP mode. Validate event->len before use: reject a length that underflows the header or that would place the IEs outside the event_body[] buffer the event was copied into. event->len here is struct mwifiex_assoc_event.len, a payload field internal to this event, not the transport frame length, so it is validated in this handler rather than at the generic MWIFIEX_TYPE_EVENT receive path, which only sees the event cause and the transport frame length. The bound is against event_body[MAX_EVENT_SIZE] rather than the actually-received length because the transports store the event differently (USB and SDIO leave the 4-byte event header in event_skb, PCIe strips it via skb_pull), whereas event_body is the single fixed buffer all of them copy the event into. This is the event-path analogue of the receive-path bounds checks added in commit 119585281617 ("wifi: mwifiex: Fix OOB and integer underflow when rx packets").			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/amd: Wait for completion instead of returning early in iommu_completion_wait() need_sync is a per-IOMMU flag shared by all domains and devices behind that IOMMU. It is set whenever a command is queued with sync == true and cleared when a completion-wait (CWAIT) command is queued. However, a cleared need_sync only means that a covering CWAIT has been queued, not that all previously queued commands have actually completed in hardware. iommu_completion_wait() read need_sync locklessly and returned early when it was false. This breaks the "block until all previously queued commands have completed" contract in a multi-CPU scenario: CPU2: queue inv-B => need_sync = true CPU1: queue CWAIT(N); need_sync = false; then wait_on_sem(N) CPU2: read need_sync == false => return 0 (no wait!) CPU2 returns without waiting for any sequence number even though its inv-B may not have completed yet (CWAIT(N), queued after inv-B, has not been signaled). CPU2 then proceeds to, for example, free page-table pages while the IOMMU can still walk stale translations, opening a use-after-free window. This is a logical race in the meaning of the flag, not a memory-visibility issue, so barriers alone do not help. Fix it without losing the optimization of avoiding redundant CWAIT commands: take iommu->lock before testing need_sync, and when it is false do not return early but wait for the last allocated sequence number (cmd_sem_val). Since need_sync == false implies no sync command was queued after the last CWAIT, that CWAIT is FIFO-ordered after every not-yet-completed command, so waiting for its sequence number guarantees all prior commands (possibly queued by another CPU) have completed. The common path with pending work is unchanged and no extra hardware command is issued.	2026-08-10	8.8	CVE-2026-68329
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ovpn: fix use after free in unlock_ovpn() unlock_ovpn() iterates over the release_list using llist_for_each_entry() and drops the peer reference inside the loop body via ovpn_peer_put(). If this drops the last reference, the peer is eventually freed. However, llist_for_each_entry() reads peer->release_entry.next in the loop advance expression, which runs after the body. By that time the peer may have already been freed, resulting in a use after free when advancing to the next list entry. Fix this by using llist_for_each_entry_safe(), which caches the next pointer before executing the loop body.	2026-08-10	8.8	CVE-2026-68341
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath6kl: fix OOB read from firmware IE lengths in connect event The firmware-controlled beacon_ie_len, assoc_req_len, and assoc_resp_len fields in ath6kl_wmi_connect_event_rx() are not validated against the buffer length. Their sum (up to 765) can exceed the actual WMI event data, causing out-of-bounds reads during IE parsing and state corruption of wmi->is_wmm_enabled. Add a check that the total IE length fits within the buffer.	2026-08-10	8.3	CVE-2026-68352
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath6kl: fix OOB read from firmware num_msg in TX complete handler The firmware-controlled num_msg field (u8, 0-255) drives the loop in ath6kl_wmi_tx_complete_event_rx() without validation against the buffer length. This allows out-of-bounds reads of up to 1020 bytes past the WMI event buffer when the firmware sends an inflated num_msg. Add a check that the buffer is large enough to hold the fixed struct and the num_msg variable-length entries.	2026-08-10	8.1	CVE-2026-68353

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: firewire: net: Fix fragmented datagram reassembly fwnet_frag_new() keeps a sorted list of received fragments for a partial datagram. When a new fragment is adjacent to an existing fragment, the code checks whether the new fragment also closes the gap to the next or previous list entry. Those neighbor lookups currently assume that the current fragment always has a real next or previous fragment. At a list edge, the next or previous entry is the list head, not a struct fwnet_fragment_info. The gap checks also compare against the old edge of the current fragment instead of the edge after adding the new fragment. As a result, a fragment that bridges two existing ranges may leave two adjacent ranges unmerged, so fwnet_pd_is_complete() can miss a complete datagram. Check for the list head before looking up the neighboring fragment, and compare the neighbor against the new fragment's far edge when deciding whether to merge all three ranges. This issue was found by a static analysis checker and confirmed by manual source review.	2026-08-10	8.8	CVE-2026-68354
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: usb: musb: omap2430: Do not put borrowed of_node in probe omap2430_probe() stores pdev->dev.of_node in a local np variable. This is a borrowed pointer and the probe function does not take a reference to it. The success and error paths nevertheless call of_node_put(np). This drops a reference that is owned by the platform device, and can leave pdev->dev.of_node with an unbalanced reference count. Do not put the borrowed platform device node from omap2430_probe(). References taken for the child USB device are handled by the device core, and the ctrl-module phandle reference is still released separately.	2026-08-10	8.4	CVE-2026-68371
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: at76c50x-usb: avoid length underflow in at76_guess_freq() at76_guess_freq() checks only that the received frame is at least a bare 802.11 header (24 bytes) before subtracting the fixed management-body offset: len -= el_off; For both beacon and probe response frames, el_off is 36. If the frame is shorter than el_off, subtracting it causes the calculated IE length to wrap. The length is eventually passed to cfg80211_find_elem_match() as a very large unsigned value, so the element walk runs beyond the RX skb. This path is reached from at76_rx_tasklet() while scanning. If the device delivers a truncated beacon or probe response, the oversized IE length causes an out-of-bounds read during scanning. Skip the IE lookup if the frame does not reach the variable elements, before subtracting el_off.	2026-08-10	8.1	CVE-2026-68373
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: fix auth_hmacs array size in struct sctp_cookie The auth_hmacs array in struct sctp_cookie is supposed to store a complete SCTP_AUTH_HMAC_ALGO parameter, which consists of a struct sctp_paramhdr followed by N HMAC identifiers. However, the array size was calculated using an extra 2 bytes instead of sizeof(struct sctp_paramhdr), which is 4 bytes. When four HMAC identifiers are configured, the HMAC-ALGO parameter stored in the endpoint is larger than the auth_hmacs buffer in the cookie. As a result, sctp_association_init() copies beyond the end of auth_hmacs when initializing the association, corrupting the adjacent auth_chunks field. This can lead to an invalid HMAC identifier being accepted and later cause an out-of-bounds read in sctp_auth_get_hmac(). Fix the array size calculation by including the full SCTP parameter header size.	2026-08-10	8.1	CVE-2026-68376
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_qca: Clear memdump state on invalid dump size qca_controller_memdump() allocates qca->qca_memdump before processing the first dump packet. For a sequence-zero packet it then disables IBS, marks memdump collection active, and reads the advertised dump size. If the controller reports a zero dump size, the error path frees the local qca_memdump object and returns without clearing qca->qca_memdump or undoing the collection state. A later memdump work item initializes its local pointer from qca->qca_memdump and skips allocation when that pointer is non-NULL, so it can operate on freed memory. The stale collection and IBS-disabled flags can also leave waiters or later transmit handling blocked behind an aborted dump. Clear the saved pointer and memdump state before returning from the invalid-size path, matching the cleanup used when hci_devcd_init() fails. A static analysis checker reported the stale memdump state, and manual source review confirmed the invalid-size failure path.	2026-08-10	8.8	CVE-2026-68389
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: hold hdev->lock for hci_conn_params lookups hci_conn_params_lookup	2026-08-10	8.8	CVE-2026-68390

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	requires hdev->lock be held, otherwise the list iteration or param access is not safe. Hold hdev->lock for params lookups in hci_sync.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: extend conn_hash lookup critical sections Using RCU-protected pointers outside the critical sections without refcount is incorrect and may result to UAF. Extend critical section to cover both hci_conn_hash lookup and use of the returned conn. Add surrounding rcu_read_lock() also when return value is not used, in preparation for RCU lockdep requirement to hci_lookup_le_connect(). This avoids concurrent deletion of the conn before we are done dereferencing it. Also, make sure to hold hdev->lock when accessing hdev->accept_list.	2026-08-10	8.8	CVE-2026-68393
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/iucv: take a reference on the socket found in afiucv_hs_rcv() afiucv_hs_rcv() looks up the destination socket under iucv_sk_list.lock, drops the lock, and then passes the socket to the afiucv_hs_callback_*() handlers without holding a reference. AF_IUCV sockets are not RCU-protected and are freed synchronously by iucv_sock_kill() -> sock_put(), so a concurrent close can free the socket in the window between read_unlock() and the handler, which then dereferences freed memory (for example sk->sk_data_ready() in afiucv_hs_callback_syn()). Take a reference with sock_hold() while the socket is still on the list and release it with sock_put() once the handler has run.	2026-08-10	8.8	CVE-2026-68397
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: defer link RX stats percpu free to RCU sta_remove_link() frees a removed MLO link's RX stats percpu buffer right away, but defers only the link container to RCU: sta_info_free_link(&alloc->info); kfree_rcu(alloc, rcu_head); The RX fast path reads link_sta under rcu_read_lock and writes the percpu stats. A reader that resolved link_sta before the removal keeps the pointer. The container stays alive from the kfree_rcu, so the read still works. But the percpu block it points to is already freed. This needs uses_rss. That is when pcpu_rx_stats exists. The full STA teardown frees the deflink stats only after synchronize_net(). The link removal path had no such barrier. The race is hard to win in practice, but the free should still wait for RCU. Free the link together with its data from a single RCU callback, so the percpu block is reclaimed only after readers drain.	2026-08-10	8.8	CVE-2026-68409
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: require CAP_NET_ADMIN in the device netns for changelink A tunnel changelink() operates on at most two netns, dev_net(dev) and the sticky underlay netns vxlan->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in vxlan->net can rewrite a vxlan device whose underlay lives in vxlan->net. vxlan_changelink() validates and applies the new configuration against vxlan->net (vxlan_config_validate(vxlan->net, ...)) and can reopen the underlay socket in that netns, so the same reasoning as the tunnel changelink series applies here. Gate vxlan_changelink() with rtnl_dev_link_net_capable(), at the top of the op before any attribute is parsed, matching ipgre_changelink() and the rest of the "require CAP_NET_ADMIN in the device netns for changelink" series. Found by Osec automated security-research tooling (https://Osec.ai).	2026-08-12	8.8	CVE-2026-68432
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: bound get_version reply decode to front len handle_get_version_reply() uses msg->front_alloc_len as the decode boundary for MON_GET_VERSION_REPLY. That is the size of the reused reply buffer, not the number of bytes actually received. A truncated reply can therefore pass ceph_decode_need() and decode the second u64 from stale tail bytes left in the buffer by an earlier message, causing an uninitialized memory read. Use msg->front.iov_len as the receive-side decode boundary, matching other libceph reply handlers and limiting decoding to the bytes that were actually read from the wire.	2026-08-12	8.6	CVE-2026-68433
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: pci: Fix handling of AIF enable without AISB When a guest seeks to register IRQs without a summary bit specified, ensure that the associated GAITE then stores 0 for the guest AISB location instead of virt_to_phys(page_address(NULL)).	2026-08-13	8.8	CVE-2026-68454
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: lpc32xx_slc: fail DMA transfer on completion timeout lpc32xx_xmit_dma() waits for the DMA completion callback but ignores wait_for_completion_timeout(). A timed out DMA transfer is therefore unmapped and reported as successful to the NAND read/write path. Return -ETIMEDOUT when the completion wait expires.	2026-08-15	8.8	CVE-2026-68466

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Terminate the DMA channel before unmapping the scatterlist so the timed out transfer cannot continue to access the buffer after the error is returned.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: validate extension-frame layout before RX Extension frames only have the extension header at the regular 802.11 header offset. The generic RX path can still reach helpers and interface dispatch code that read regular header address fields before unsupported extension subtypes are dropped. mac80211 currently only handles S1G beacon extension frames. Drop other extension subtypes before they can reach regular-header RX processing. For S1G beacons, linearize the SKB with the management-frame path and require the fixed S1G beacon header, including optional fixed fields indicated by frame control, before generic RX dispatch. Route S1G beacons through the station/default-link RX path without regular-header station lookup. Avoid regular-header address reads in the mac80211 RX paths that process S1G extension beacons, including accept-frame, duplicate-detection, address-copy, and MLO address-translation paths. Also make ieee80211_get_bssid() length-safe before returning the S1G source-address pointer.	2026-08-15	8.8	CVE-2026-68470
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ieee80211: validate MLE common info length ieee80211_mle_common_size() uses the first common-info octet as the common information length for all known MLE types. However, ieee80211_mle_size_ok() only validates that octet for Basic, Probe Request, and TDLS MLEs. Reconfiguration MLEs also skipped the length octet when calculating the minimum common size, and Priority Access MLEs skipped validation of the advertised common information length. Account for the Reconfiguration common-info length octet and validate the advertised common information length for all known MLE types. Keep unknown-type handling unchanged. [remove now misleading comment]	2026-08-15	8.8	CVE-2026-68471
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: validate EHT MLE before MLD ID read cfg80211_gen_new_ie() copies ML probe response elements from the parent frame when the parent EHT multi-link element has an MLD ID matching the nontransmitted BSSID index. The code only checked that the extension element had more than one byte before calling ieee80211_mle_get_mld_id(). That helper assumes a BASIC MLE with enough common info and documents that callers must first use ieee80211_mle_type_ok(). Attack chain: malicious AP sends a short EHT MLE in an MBSSID beacon. cfg80211_inform_bss_frame_data() stores the copied IE buffer. cfg80211_parse_mbssid_data() builds the nontransmitted BSS IE. cfg80211_gen_new_ie() sees the EHT MLE in the parent frame. ieee80211_mle_get_mld_id() then reads past the IE boundary. Validate the MLE type and size before reading the MLD ID. This matches the contract required by the MLE helper and rejects the short element before any internal MLE fields are accessed.	2026-08-15	8.1	CVE-2026-68472
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: cyw: fix heap overflow on a short auth frame brcmf_notify_auth_frame_rx() takes the frame length from the firmware event and copies the frame body with the management header offset subtracted: u32 mgmt_frame_len = e->datalen - sizeof(struct brcmf_rx_mgmt_data); ... memcpy(&mgmt_frame->u, frame, mgmt_frame_len - offsetof(struct ieee80211_mgmt, u)); The only length check is e->datalen >= sizeof(*rxframe), so mgmt_frame_len can be anything from 0 up. offsetof(struct ieee80211_mgmt, u) is 24. When mgmt_frame_len is below that, the subtraction wraps as an unsigned value to a huge length. The memcpy then runs far past the kzalloc'd buffer. A malicious or malfunctioning AP can make the frame short during the external SAE auth exchange, so this is a remotely triggered heap overflow. Reject frames shorter than the management header offset before the copy.	2026-08-15	8.8	CVE-2026-72003
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: use parsed transport offset in SCTP state lookup set_sctp_state() reads the SCTP chunk header again in order to drive the IPVS SCTP state table. For IPv6 it computes the offset with sizeof(struct ipv6hdr), while the surrounding IPVS code uses iph.len from ip_vs_fill_iph_skb(), where ipv6_find_hdr() has already skipped extension headers and found the real transport header. This makes the state machine read from the wrong offset for IPv6 SCTP packets that carry extension headers. For example, an INIT packet with an 8-byte destination options header can be scheduled correctly by sctp_conn_schedule(), but set_sctp_state() reads the first byte of the SCTP verification tag as a DATA chunk type. The connection then moves from NONE to	2026-08-15	8.2	CVE-2026-72021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ESTABLISHED instead of INIT1, gets the longer established timeout, and updates the active/inactive destination counters incorrectly. This happens even though the SCTP handshake has not completed. Use the parsed transport offset passed down from ip_vs_set_state() for the SCTP chunk-header lookup. For IPv4 and IPv6 packets without extension headers this preserves the existing offset.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: wwan: iosm: bound device offsets in the MUX downlink decoder mux_dl_adb_decode() walks a chain of aggregated datagram tables using offsets and lengths taken from the modem. first_table_index, next_table_index, table_length, datagram_index and datagram_length are all device supplied le values. Only first_table_index was checked, and only for being non zero. The decoder then formed adth = block + adth_index and read the table header and the datagram entries with no bound against the received skb. A modem that reports an index or a length past the downlink buffer makes the decoder read out of bounds. The buffer is IPC_MEM_MAX_DL_MUX_LITE_BUF_SIZE and skb->len is at most that, so skb->len is the real limit, but none of these in band offsets were checked against it. The table chain is also followed with no forward progress check. The loop takes the next table from adth->next_table_index and stops only when that reaches zero. A modem can stage two tables that point at each other, so the loop never ends. It runs in softirq and clones the skb on every pass. Validate every device offset and length against skb->len before use. The block header must fit. Each table header, on entry and after every next_table_index, must lie inside the skb. The datagram table must fit. Each datagram index and length must stay inside the skb. The header padding must not exceed the datagram length so the receive length does not wrap. Require each next_table_index to move forward so the chain cannot cycle. This was reproduced under KASAN as a slab out of bounds read on a normal downlink receive once the iosm net device is up.	2026-08-15	8.8	CVE-2026-72029
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_taprio: Replace direct dequeue call with peek and qdisc_dequeue_peeked When taprio's software path peeks a non-work-conserving child qdisc, the child stashes the peeked skb in its gso_skb; taprio_dequeue_from_txq() then takes the packet with a direct child ->dequeue() call, which ignores that stash, orphans the peeked skb and desyncs the child's qlen/backlog. With a qfq child this re-enters the child on an emptied list and dereferences NULL, panicking the kernel from softirq on ordinary egress. Take the packet through qdisc_dequeue_peeked(), as sch_red and sch_sfb now do. The helper returns the child's stashed skb first and is a no-op when there is none, so a work-conserving child is unaffected and the gated path now consumes the skb whose length was charged to the budget.	2026-08-15	8.2	CVE-2026-72035
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: cn10k: restrict VF LMTLINE sharing to its own PF rvu_mbox_handler_lmtst_tbl_setup() uses req->base_pcifunc as a direct index into the LMT map table to read another function's LMTLINE physical base address and copy it into the caller's own LMT map table entry. The mailbox dispatcher authenticates req->hdr.pcifunc from the IRQ source, but req->base_pcifunc is a separate payload field and is not sanitized. Reject the request with -EPERM when a VF caller's base_pcifunc is not a valid function under its own PF. is_pf_func_valid() bounds the FUNC field to the PF's configured VF count, keeping the computed index inside the caller's own slot block.	2026-08-15	8.8	CVE-2026-72045
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ip6_tunnel: require CAP_NET_ADMIN in the device netns for changelink ip6_tnl_changelink() operates on at most two netns, dev_net(dev) and the tunnel link netns t->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in t->net can rewrite a tunnel that lives in t->net. Gate ip6_tnl_changelink() on rtnl_dev_link_net_capable() at its top, before any attribute is parsed.	2026-08-15	8.8	CVE-2026-72051
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ip6_gre: require CAP_NET_ADMIN in the device netns for changelink ip6gre_changelink() and ip6erspan_changelink() operate on at most two netns, dev_net(dev) and the tunnel link netns t->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in t->net can rewrite a tunnel that lives in t->net. Gate both ops on rtnl_dev_link_net_capable() at their top, before any attribute is parsed.	2026-08-15	8.8	CVE-2026-72052

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ipip: require CAP_NET_ADMIN in the device netns for changelink ipip_changelink() operates on at most two netns, dev_net(dev) and the tunnel link netns t->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in t->net can rewrite a tunnel that lives in t->net. Gate ipip_changelink() on rtnl_dev_link_net_capable() at its top, before any attribute is parsed.	2026-08-15	8.8	CVE-2026-72053
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ip_vti: require CAP_NET_ADMIN in the device netns for changelink vti_changelink() operates on at most two netns, dev_net(dev) and the tunnel link netns t->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in t->net can rewrite a tunnel that lives in t->net. Gate vti_changelink() on rtnl_dev_link_net_capable() at its top, before any attribute is parsed.	2026-08-15	8.8	CVE-2026-72054
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ip6_vti: require CAP_NET_ADMIN in the device netns for changelink vti6_changelink() operates on at most two netns, dev_net(dev) and the tunnel link netns t->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in t->net can rewrite a tunnel that lives in t->net. Gate vti6_changelink() on rtnl_dev_link_net_capable() at its top, before any attribute is parsed.	2026-08-15	8.8	CVE-2026-72055
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_ct: preserve tc_skb_cb across defragmentation tcf_ct_handle_fragments() calls nf_ct_handle_fragments() without saving and restoring skb->cb. The defrag helper clears IPCB/IP6CB, which aliases the tc_skb_cb/qdisc_skb_cb control buffer. Fragmented traffic through act_ct therefore loses qdisc metadata such as pkt_segs and can trigger WARN_ON_ONCE() in qdisc_pkt_segs() when panic_on_warn is enabled. Save and restore the full tc_skb_cb around nf_ct_handle_fragments(), matching the pattern used by ovs_ct_handle_fragments().	2026-08-15	8.2	CVE-2026-72057
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: sit: require CAP_NET_ADMIN in the device netns for changelink ipip6_changelink() operates on at most two netns, dev_net(dev) and the tunnel link netns t->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in t->net can rewrite a tunnel that lives in t->net. Gate ipip6_changelink() on rtnl_dev_link_net_capable() at its top, before any attribute is parsed. sit was the one tunnel type not covered by the recent series that added this check to the other changelink() handlers.	2026-08-15	8.8	CVE-2026-72061
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm-integrity: fix a bug if the bio is out of limits If dm_integrity_check_limits fails, the code would exit with DM_MAPO_KILL. However, the range would be already locked at this point, and it wouldn't be unlocked, resulting in a deadlock. Let's move the limit check up, so that when it exits, no resources are leaked.	2026-08-15	8.8	CVE-2026-72100
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm era: fix out-of-bounds memory access for non-zero start sector dm-era tracks writes in target-relative blocks, but era_map() calculates the writeset block before applying the target offset. Tables with a non-zero start sector can therefore pass an absolute mapped-device block to metadata_current_marked(). If the absolute block is beyond the current writeset size, writeset_marked() tests past the end of the in-core bitset. KASAN reports this as a vmalloc-out-of-bounds access. Apply the target offset before calculating the era block so writeset lookups use the target-relative block number.	2026-08-15	8.8	CVE-2026-72107
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Reset register bounds before narrowing retval range in check_mem_access() When the BPF verifier processes a context load of an LSM hook return value, it calls __mark_reg_s32_range() to narrow the register to the hook's valid range. However, __mark_reg_s32_range() intersects the new range with the register's existing bounds using max_t()/min_t() rather than replacing them. If the destination register carries stale bounds from a prior instruction (e.g. BPF_MOV64_IMM), the intersection can produce a range narrower than reality. The verifier then believes it knows the register's exact value, while at runtime the	2026-08-15	8.8	CVE-2026-72111

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	actual hook return value is loaded, creating a verifier/runtime mismatch that can be used to bypass BPF memory safety checks. The else branch already calls mark_reg_unknown() to reset register state before any narrowing. Apply the same reset in the is_retval path so stale bounds are cleared before __mark_reg_s32_range() intersects.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: track a single source interface for ANYDEV timeout/throttle ops An ANYDEV rx op (ifindex == 0) with an active RX timeout and/or throttle timer has no defined semantics when matching frames arrive from several interfaces: bcm_rx_handler() can run concurrently for the same op on different CPUs, racing hrtimer_cancel()/bcm_rx_starttimer() against bcm_rx_timeout_handler() and causing spurious RX_TIMEOUT notifications and last_frames corruption. The same concurrency lets throttled multiplex frames from different interfaces clobber the single rx_ifindex/rx_stamp fields shared by the op. Add op->if_detected to track the first interface that delivers a matching frame while a timeout/throttle timer is configured, and reject frames from any other interface for that op. The claim is decided in bcm_rx_handler() before hrtimer_cancel() touches op->timer, so a rejected frame can never disturb the claimed interface's watchdog. RTR-mode ops are excluded via RX_RTR_FRAME, independent of kt_ival1/kt_ival2, since those may briefly hold a stale value from an earlier non-RTR configuration. The claim is released in bcm_notify() on NETDEV_UNREGISTER and in bcm_rx_setup() when SETTIMER reconfigures the timer values. A (re-)claim is only possible on CAN devices in NETREG_REGISTERED dev->reg_state to cover the release in bcm_notify() where reg_state becomes NETREG_UNREGISTERING until synchronize_net().	2026-08-15	8.1	CVE-2026-72115
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: add locking when updating filter and timer values KCSAN detected a simultaneous access to timer values that can be overwritten in bcm_rx_setup() when updating timer and filter content while bcm_rx_handler(), bcm_rx_timeout_handler() or bcm_rx_thr_handler() run concurrently on incoming CAN traffic. Protect the timer (ival1/ival2/kt_ival1/kt_ival2/kt_lastmsg) and filter (nframes/flags/frames/last_frames) updates in bcm_rx_setup() with a new per-op bcm_rx_update_lock, taken with the matching scope in the RX handlers. memcpy_from_msg() is staged into a temporary buffer before the lock is taken, since it can sleep and must not run under a spinlock. hrtimer_cancel() is always called without bcm_rx_update_lock held, since bcm_rx_timeout_handler()/bcm_rx_thr_handler() take the same lock and a running callback would otherwise deadlock against the canceller. Also close a related race: bcm_rx_setup() cleared the RTR flag in the stored reply frame's can_id as a separate, unprotected step after the frame content was already installed, so a concurrent bcm_rx_handler() could transmit a stale reply with CAN_RTR_FLAG still set. Fold that normalization into the initial frame preparation instead (on the staged buffer for updates, directly on op->frames pre-registration for new ops), so the installed frame is always atomically self-consistent. bcm_rx_handler()'s RX_RTR_FRAME check now takes a lock-protected snapshot of op->flags before deciding whether to call bcm_can_tx(), but does not hold the lock across that call. Also take a lock-protected snapshot of the currframe in bcm_can_tx() to avoid partly overwrites by content updates in bcm_tx_setup(). Finally check if a TX_RESET_MULTI_IDX/SETTIMER might have reset op->currframe between the two locked sections in bcm_can_tx(). Omit calling hrtimer_forward() with zero interval in bcm_rx_thr_handler(). kt_ival2 may have been concurrently cleared by bcm_rx_setup() before it cancels this timer, so check kt_ival2 inside the bcm_rx_update_lock.	2026-08-15	8.8	CVE-2026-72121
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: isotp: serialize TX state transitions under so->rx_lock The TX state machine (so->tx.state) is driven from three contexts: sendmsg() claiming and progressing a transfer, the RX path consuming Flow Control/echo frames, and two hrtimers timing out a stalled transfer. Mixing a lock-free cmpxchg() claim in sendmsg() with hrtimer_cancel() calls made under so->rx_lock elsewhere left windows where a frame or timer callback could act on a state that had already moved on, corrupting an unrelated transfer. so->rx_lock now covers the full lifecycle of a TX claim: sendmsg() takes it to check so->tx.state is ISOTP_IDLE, switch it to ISOTP_SENDING, bump so->tx_gen and drain the previous transfer's timers - all as one critical section. isotp_rcv_fc()/isotp_rcv_cf() already run under this lock via isotp_rcv(), and isotp_rcv_echo() now takes it itself, so none of them can ever observe a	2026-08-15	8.8	CVE-2026-72124

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	transfer mid-claim. This also means a transfer can no longer be handed to sendmsg()'s cleanup paths (signal or send error) while another thread is concurrently claiming or finishing it, so those paths can cancel timers and reset the state unconditionally. isotp_release() claims the socket the same way, so a racing sendmsg() sees a consistent ISOTP_SHUTDOWN and skips arming its timer or sending. Only the hrtimer callbacks stay outside so->rx_lock, since they run under so->rx_lock's cancellation elsewhere and taking it themselves would deadlock. so->tx_gen lets them recognize whether the transfer they timed out is still the one currently active, so they don't report an error against a transfer that has since completed or been superseded.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: spi: uniphier: Fix completion initialization order before devm_request_irq() The driver calls devm_request_irq() before initializing the completion used by the interrupt handler. Because the interrupt may occur immediately after devm_request_irq(), the handler may execute before init_completion(). This may result in calling complete() on an uninitialized completion, causing undefined behavior. This has been observed with KASAN. Fix this by initializing the completion before registering the IRQ.	2026-08-15	8.4	CVE-2026-72133
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: xfrm_interface: require CAP_NET_ADMIN in the device netns for changelink xfrm_changelink() operates on at most two netns, dev_net(dev) and the interface link netns xi->net. They differ once the device is created in or moved to a netns other than the one the request runs in. The rtnl changelink path checks CAP_NET_ADMIN only against dev_net(dev), so a caller privileged there but not in xi->net can rewrite an interface that lives in xi->net. Gate xfrm_changelink() on rtnl_dev_link_net_capable() at its top, before any attribute is parsed.	2026-08-15	8.8	CVE-2026-72136
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dmaengine: sh: rz-dmac: Move interrupt request after everything is set up Once the interrupt is requested, the interrupt handler may run immediately. Since the IRQ handler can access channel->ch_base, which is initialized only after requesting the IRQ, this may lead to invalid memory access. Likewise, the IRQ thread may access uninitialized data (the ld_free, ld_queue, and ld_active lists), which may also lead to issues. Request the interrupts only after everything is set up. To keep the error path simpler, use dmam_alloc_coherent() instead of dma_alloc_coherent().	2026-08-15	8.4	CVE-2026-72146
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dmaengine: dw-edma: Add spinlock to protect DONE_INT_MASK and ABORT_INT_MASK The DONE_INT_MASK and ABORT_INT_MASK registers are shared by all DMA channels, and modifying them requires a read-modify-write sequence. Because this operation is not atomic, concurrent calls to dw_edma_v0_core_start() can introduce race conditions if two channels update these registers simultaneously. Add a spinlock to serialize access to these registers and prevent race conditions. [den: update dw_edma.lock comment]	2026-08-15	8.8	CVE-2026-72148
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tpm: tpm2-sessions: wait for async KPP completion in tpm_buf_append_salt tpm_buf_append_salt() in drivers/char/tpm/tpm2-sessions.c calls crypto_kpp_generate_public_key() and crypto_kpp_compute_shared_secret() without installing a completion callback, discards both return values, and immediately frees the kpp_request via kpp_request_free(). When the resolved ecdh-nist-p256 KPP backend is asynchronous (atmel-ecc, HPRE, keembay-ocs), either operation returns -EINPROGRESS and the deferred completion worker dereferences the freed request. The path fires automatically from the hwrng_fillfn kernel thread via tpm_get_random -> tpm2_get_random -> tpm2_start_auth_session -> tpm_buf_append_salt on every entropy poll, without any userland action. Install crypto_req_done as the completion callback, wrap both KPP operations in crypto_wait_req(), and propagate errors to the caller. The wait is a no-op for synchronous backends.	2026-08-15	8.4	CVE-2026-72151
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: thunderbolt: Fix frags[] overflow by bounding frame_count tbneth_poll() assembles a multi-frame ThunderboltIP packet into one skb. The first frame goes into the skb linear area and every further frame is added as a page fragment. skb_add_rx_frag(skb, skb_shinfo(skb)->nr_frags, page, hdr_size, frame_size, TBNETH_RX_PAGE_SIZE - hdr_size); A packet of frame_count frames therefore ends up with frame_count - 1 fragments. tbneth_check_frame() only bounds the peer supplied frame_count to TBNETH_RING_SIZE / 4 (64), which is far above MAX_SKB_FRAGS (17 by default). A	2026-08-15	8.8	CVE-2026-72157

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	peer that sends a packet of 19 or more small frames pushes nr_frags past MAX_SKB_FRAGS, so skb_add_rx_frag() writes past skb_shinfo()->frags[] and corrupts memory after the shared info. Tighten the start of packet bound to MAX_SKB_FRAGS + 1 so a packet can never produce more fragments than frags[] can hold. This matches the recent skb frags overflow fixes in other receive paths, for example f0813bcd2d9d ("net: wwan: t7xx: fix potential skb->frags overflow in RX path") and 600dc40554dc ("net: usb: cdc-phonet: fix skb frags[] overflow in rx_complete()).			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: reject dinodes with non-canonical i_mode type Patch series "ocfs2: harden inode validators against forged metadata", v2. This series adds three structural checks to OCFS2 dinode validation so malformed on-disk fields are rejected before ocfs2_populate_inode() copies them into the in-core inode. The checks cover: - i_mode values whose type bits do not name a canonical POSIX file type; - non-device dinodes whose id1.dev1.i_rdev field is non-zero; and - non-inline dinodes that claim non-zero i_size while i_clusters is zero, covering directories unconditionally and regular files on non-sparse volumes. The normal read path reports these through ocfs2_error(), matching the existing suballoc-slot, inline-data, chain-list, and refcount checks. The online filecheck path uses the same structural predicates but keeps its own reporting contract, returning OCFS2_FILECHECK_ERR_INVALIDINO instead of calling ocfs2_error(). This patch (of 3): ocfs2_validate_inode_block() currently accepts any non-zero i_mode value. ocfs2_populate_inode() then copies that mode verbatim into inode->i_mode and dispatches on i_mode & S_IFMT to the file/dir/symlink/special_file iops; an unrecognised type falls through to ocfs2_special_file_iops and init_special_inode(). Reject dinodes whose type bits do not name one of the seven canonical POSIX file types. Use fs_umode_to_ftype(), the same generic file-type conversion helper OCFS2 already uses for directory entries, so the accepted inode type set matches the kernel file-type vocabulary instead of open-coding a local switch. Apply the same structural check to the online filecheck read path. filecheck keeps its own error namespace, so it reports malformed i_mode through the filecheck logger and OCFS2_FILECHECK_ERR_INVALIDINO instead of calling ocfs2_error(), but it must not allow a malformed dinode to proceed into ocfs2_populate_inode().	2026-08-15	8.8	CVE-2026-72160
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: landlock: Fix LANDLOCK_SCOPE_SIGNAL bypass on the SIGIO path LANDLOCK_SCOPE_SIGNAL must prevent a sandboxed process from signaling processes outside its Landlock domain. It can be bypassed through the asynchronous SIGIO delivery path. A sandboxed process that owns any file or socket can arm it with fcntl(fd, F_SETOWN, -pgid), fcntl(fd, F_SETSIG, SIGKILL) and O_ASYNC, so that an I/O event makes the kernel deliver the chosen signal to the whole process group. As the head of its process group's task list (the default position right after fork()) that group can also hold the non-sandboxed process that launched it, e.g. a supervisor or a security monitor. The sandbox can thus kill or signal the processes LANDLOCK_SCOPE_SIGNAL is meant to protect from it. The scope is enforced in hook_file_send_sigiotask() against the Landlock domain recorded at F_SETOWN time, not the live domain of the sender. control_current_fowner() decides whether to record that domain and skips recording it when the fowner target is in the caller's thread group, which is safe only for a single-task target (PIDTYPE_PID, PIDTYPE_TGID). For a process group (PIDTYPE_PGID) pid_task() returns only one member; recording is skipped whenever that member shares the caller's thread group, and hook_file_send_sigiotask() then lets the signal fan out to the whole group unchecked. Record the domain for every non single-process target so the scope is enforced against each group member at delivery time. That recording is necessary but not sufficient on its own: the kernel signals a process group through its members' thread-group leaders, and the leader of the registrant's own process can carry a different Landlock domain than the sibling thread that armed the owner. domain_is_scoped() would then deny that leader, even though commit 18eb75f3af40 ("landlock: Always allow signals between threads of the same process") requires same-process delivery to be allowed. hook_task_kill() avoids this by evaluating same_thread_group() live, per recipient; the SIGIO path instead delegates the whole decision to a single registration-time check, which a process-group fan-out cannot honor. So also record the registrant's thread group next to its domain and exempt it at delivery: hook_file_send_sigiotask() allows the signal whenever the recipient belongs to the registrant's own process, restoring the same-process guarantee while keeping out-of-domain group members blocked.	2026-08-15	8.4	CVE-2026-72183

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The direct kill() path (hook_task_kill) already evaluates the live domain and is unaffected. [mic: Check pid_type earlier and improve comment, fix commit message, fix comment formatting]			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: bound copy_lcms dp->page_lcms[] index in analysis pass In log_replay()'s analysis pass, after find_dp() returns a valid DIR_PAGE_ENTRY for the (target_attr, target_vcn) tuple, the copy_lcms block walks lrh->lcms_follow further entries: t16 = le16_to_cpu(lrh->lcms_follow); for (i = 0; i < t16; i++) { size_t j = (size_t)(le64_to_cpu(lrh->target_vcn) - le64_to_cpu(dp->vcn)); dp->page_lcms[j + i] = lrh->page_lcms[i]; } find_dp() only validates that target_vcn falls within [dp->vcn, dp->vcn + dp->lcms_follow], i.e., that the FIRST cluster is covered. The walk through the further entries is not bounded against dp->lcms_follow. For a malformed LRH where target_vcn = dp->vcn + dp->lcms_follow - 1 and lrh->lcms_follow > 1, the i > 0 writes overflow the dp's allocated page_lcms[] array. Add the missing j + lrh->lcms_follow <= dp->lcms_follow guard. Reproduced under UML+KASAN on mainline 8d90b09e6741 as a slab-out-of-bounds write of size 8 from log_replay+0x68d4 on the mount path. This is distinct from Pavitra Jha's 2026-05-02 patch ("fs/ntfs3: validate lcms_follow in log_replay conversion", <20260502154252.164586-1-jhapavitra98@gmail.com>) which addresses the separate version-0 dirty-page-table conversion path's memmove(&dp->vcn, ...) call. The two fixes are complementary; both should land. [almaz.alexandrovich@paragon-software.com: clang-formatted the changes, fixed conflicts]	2026-08-15	8.4	CVE-2026-72196
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: bound DeleteIndexEntryAllocation memmove length In do_action()'s DeleteIndexEntryAllocation case, e->size comes from an on-disk INDEX_BUFFER entry. When e->size makes e + e->size point past hdr + hdr->used, PtrOffset(e1, Add2Ptr(hdr, used)) returns a negative ptrdiff_t that is silently cast to a quasi-infinite size_t when passed to memmove(). The memmove then walks past the destination buffer. The sibling DeleteIndexEntryRoot case at fslog.c:3540-3543 already carries the corresponding guard: if (PtrOffset(e1, Add2Ptr(hdr, used)) < esize Add2Ptr(e, esize) > Add2Ptr(lrh, rec_len) used + esize > le32_to_cpu(hdr->total)) { goto dirty_vol; } Apply the same shape to the allocation-path case. Also reject esize == 0: memmove(e, e, ...) is a no-op and leaves hdr->used unchanged, hiding a malformed entry from the existing check_index_header() walk. Reproduced under UML+KASAN on mainline 8d90b09e6741 by mounting a crafted NTFS image: the unguarded memmove takes a length of 0xfffffffff00 and the kernel oopses in memmove+0x81/0x1a0 on the do_action+0x36a2 frame. [almaz.alexandrovich@paragon-software.com: clang-formatted the changes]	2026-08-15	8.4	CVE-2026-72197
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: centralize \$INDEX_ROOT header validation Add a dedicated helper to perform stricter validation of \$INDEX_ROOT and use it for both directory inodes and named index inodes. This keeps the root size and header geometry checks consistent across both read paths.	2026-08-15	8.4	CVE-2026-72204
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: mcast: avoid OOB read of num_dests header Before the access to struct batadv_tlv_mcast_tracker's num_dests, it is attempted to check whether enough space is actually in the network header. But instead of using offsetofend() to check for the whole size (2) which must be accessible, offsetof() of is called. The latter is always returning 0. The comparison with the network header length will always return that enough data is available - even when only 1 or 0 bytes are accessible. Instead of using offsetofend(), use the more common check for the whole header.	2026-08-15	8.1	CVE-2026-72227
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: bla: reacquire gw address after skb realloc The pskb_may_pull() called by batadv_bla_is_backbone_gw() could reallocate the buffer behind the skb. Variables which were pointing to the old buffer need to be reassigned to avoid an use-after-free.	2026-08-15	8.8	CVE-2026-72233
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: retrieve ethhdr after potential skb realloc on RX pskb_may_pull() in batadv_interface_rx() could reallocate the buffer behind the skb. Variables which were pointing to the old buffer need to be reassigned to avoid an use-after-free. This was done correctly for the VLAN header but missed for the ethernet header which is later used for the TT and AP isolation handling.	2026-08-15	8.8	CVE-2026-72235

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: selinux: check connect-related permissions on TCP Fast Open Similar to Landlock, SELinux was not updated when TCP Fast Open support was introduced to ensure connect-related permissions are checked when using TCP Fast Open. Update its socket_sendmsg() hook to call selinux_socket_connect() when MSG_FASTOPEN is passed.	2026-08-15	8.4	CVE-2026-72243
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Nullify irqfd->producer if updating IRTE for bypass fails Nullify irqfd->producer if updating the IRTE for bypass fails, as leaving a dangling pointer will result in a use-after-free if the irqfd is reachable through KVM's routing, but the producer is freed separately. E.g. for VFIO PCI, the producer is embedded in struct "vfio_pci_irq_ctx" and freed when the vector is disabled, which can happen independent of routing updates. [sean: drop PPC change, massage changelog]	2026-08-15	8.8	CVE-2026-72283
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Do not allow intra-host migration/mirroring of SNP VMs The intra-host migration/mirroring feature is not fully implemented for SEV-SNP VMs. The proper migration requires additional SNP-specific state such as guest_req_mutex, guest_req_buf, and guest_resp_buf to be transferred or initialized on the destination. The SNP VM mirroring requires vmsa features to be copied as well otherwise ASID would be bound to SNP range while VM is detected as a SEV VM. Reject SNP source VMs in migration/mirroring until proper SNP state transfer is implemented. [sean: let lines poke past 80 chars, tag for stable]	2026-08-15	8.8	CVE-2026-72286
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Check irq validity in kvm_vcpu_ioctl_interrupt() Function kvm_vcpu_ioctl_interrupt() can be called from userspace, here add irq validity checking in kvm_vcpu_ioctl_interrupt().	2026-08-15	8.8	CVE-2026-72294
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: LoongArch: KVM: Validate irqchip index in irqfd routing Sashiko reported that the irqchip index is not validated for LoongArch. Add validation and reject out-of-range irqchip indexes to avoid indexing past the routing table's chip array.	2026-08-15	8.8	CVE-2026-72295
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: fix 32-bit integer overflow in qrtr_endpoint_post() qrtr_endpoint_post() validates an incoming packet with if (!size len != ALIGN(size, 4) + hdrlen) goto err; where size comes from the wire. On 32-bit, size_t is 32 bits and ALIGN(size, 4) wraps to 0 for size >= 0xffffffff, so the check passes and skb_put_data(skb, data + hdrlen, size) writes past the hdrlen-sized skb and oopses the kernel. 64-bit is unaffected. This is the 32-bit residual of ad9d24c9429e2 ("net: qrtr: fix OOB Read in qrtr_endpoint_post"), which fixed only the 64-bit case. Reject any size that cannot fit the buffer before the ALIGN.	2026-08-15	8.4	CVE-2026-72298
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix overflow in passthrough ioctl bounds check smb2_ioctl_query_info() validates the PASSTHRU_FSCTL response payload before copying it to userspace. The payload offset and length both come from 32-bit fields. The bounds check currently adds OutputOffset and qi.input_buffer_length directly, so the addition can wrap in 32-bit arithmetic before the result is compared against the response buffer length. A malicious server can use a large OutputOffset and a small OutputCount to make the wrapped sum pass the bounds check. The later copy_to_user() then reads from io_rsp + OutputOffset, outside the response buffer. Use size_add() for the offset plus length check so overflow is treated as out of bounds.	2026-08-15	8.1	CVE-2026-72310
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: fix malformed ISO_END/CONT handling Core specification (Part C vol 4 sec 5.4.5) does not exclude empty ISO_CONT, ISO_END packets. We currently reject them if they are last. If controller sends malformed sequence ISO_START -> rx_len = 4, ISO_CONT skb->len 4, ISO_START that ends payload in ISO_CONT, we leak conn->rx_skb. If controller sends too long ISO_END, we panic on skb_put. If controller sends too short ISO_END we accept it. Fix by marking unfinished ISO_START via conn->rx_skb != NULL. Check skb->len properly before skb_put. Combine the ISO_CONT/END code paths as they require the same initial checks. Reject too short ISO_END packets.	2026-08-15	8.8	CVE-2026-72334
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix HV VHCA stats agent registration race mlx5e_hv_vhca_stats_create() registers the stats agent through mlx5_hv_vhca_agent_create(). The helper publishes the agent in hv_vhca->agents[type] under agents_lock and immediately schedules an asynchronous control invalidation on the HV VHCA workqueue before returning to mlx5e. The asynchronous invalidation invokes the control agent's invalidate	2026-08-15	8.4	CVE-2026-72342

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	callback, which reads the hypervisor control block and forwards the command to <code>mlx5e_hv_vhca_stats_control()</code> . That callback may either: - call <code>cancel_delayed_work_sync(&priv->stats_agent.work)</code> , or - call <code>queue_delayed_work(priv->wq, &sagent->work, sagent->delay)</code> . However, the <code>delayed_work</code> and <code>priv->stats_agent.agent</code> are only initialized after <code>mlx5_hv_vhca_agent_create()</code> returns to <code>mlx5e</code> : <code>agent = mlx5_hv_vhca_agent_create(...); /* publish + invalidate */ ... priv->stats_agent.agent = agent; /* too late */ INIT_DELAYED_WORK(&priv->stats_agent.work, ...); /* too late */</code> If the asynchronous control path runs before the two assignments above, it can: - Operate on an uninitialized <code>delayed_work</code> whose <code>timer.function</code> is <code>NULL</code> . <code>queue_delayed_work()</code> calls <code>add_timer()</code> unconditionally, so when the timer expires the timer <code>softirq</code> invokes a <code>NULL</code> function pointer. - Re-initialize the timer later through <code>INIT_DELAYED_WORK()</code> while the timer is already enqueued in the timer wheel, corrupting the <code>hlist</code> (<code>entry.pprev</code> cleared while the previous bucket node still points at this entry). - When the worker eventually runs, <code>mlx5e_hv_vhca_stats_work()</code> reads <code>sagent->agent</code> (<code>NULL</code>) and dereferences it inside <code>mlx5_hv_vhca_agent_write()</code> . Fix this by: - Initializing <code>priv->stats_agent.work</code> before invoking <code>mlx5_hv_vhca_agent_create()</code> , so the work is always in a valid state when the control callback observes it. - Adding a struct <code>mlx5_hv_vhca_agent **ctx_update</code> out-parameter to <code>mlx5_hv_vhca_agent_create()</code> . The helper writes the agent pointer to <code>*ctx_update</code> before publishing into <code>hv_vhca->agents[]</code> and triggering the <code>agents_update</code> flow, so any callback subsequently invoked from that flow already sees a valid <code>priv->stats_agent.agent</code> . This avoids having the control callback participate in agent initialization. While at it, access <code>priv->stats_agent.agent</code> with <code>READ_ONCE()/WRITE_ONCE()</code> for the cross-CPU access with the worker, and clear <code>priv->stats_agent.buf</code> on the <code>agent_create()</code> failure path.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>net/mlx5e</code> : Fix HV VHCA stats zero-sized buffer allocation <code>mlx5e_hv_vhca_stats_create()</code> is called from <code>mlx5e_nic_enable()</code> , before <code>mlx5e_open()</code> . At that point <code>priv->stats_nch</code> is still zero, because it is only ever incremented in <code>mlx5e_channel_stats_alloc()</code> , which is reached only from <code>mlx5e_open_channel()</code> . <code>mlx5e_hv_vhca_stats_buf_size()</code> therefore returns 0, and <code>kvzalloc(0, GFP_KERNEL)</code> returns <code>ZERO_SIZE_PTR</code> (<code>(void *)16</code>) rather than <code>NULL</code> . The "if (!buf)" guard does not catch this, and <code>mlx5e_hv_vhca_stats_create()</code> completes "successfully" with <code>priv->stats_agent.buf</code> set to <code>ZERO_SIZE_PTR</code> . Once channels are opened (<code>priv->stats_nch > 0</code>) and the hypervisor enables stats reporting, <code>mlx5e_hv_vhca_stats_work()</code> recomputes <code>buf_len</code> using the new non-zero <code>stats_nch</code> and calls <code>memset(buf, 0, buf_len)</code> on <code>ZERO_SIZE_PTR</code> , faulting at address 0x10. Allocate the buffer based on <code>priv->max_nch</code> , which is set in <code>mlx5e_priv_init()</code> and is the upper bound on <code>stats_nch</code> : - Add a separate helper <code>mlx5e_hv_vhca_stats_buf_max_size()</code> that returns <code>sizeof(per_ring_stats) * max(max_nch, stats_nch)</code> , and use it for the <code>kvzalloc()</code> in <code>mlx5e_hv_vhca_stats_create()</code> . - Keep <code>mlx5e_hv_vhca_stats_buf_size()</code> (which returns based on <code>stats_nch</code>) for the worker's active payload size, so the wire format (<code>block->rings = stats_nch</code>) and the amount of data filled by <code>mlx5e_hv_vhca_fill_stats()</code> are unchanged. The <code>max(max_nch, stats_nch)</code> guard handles the rare case where <code>mlx5e_attach_netdev()</code> recomputes <code>max_nch</code> downward across a detach/resume cycle while <code>priv->stats_nch</code> persists (<code>mlx5e_detach_netdev</code> does not call <code>mlx5e_priv_cleanup</code> , so <code>stats_nch</code> is only reset when the netdev is destroyed). Without the guard, the worker could compute <code>buf_len</code> from <code>stats_nch</code> and overrun the smaller buffer allocated based on the reduced <code>max_nch</code> . Allocating a non-zero buffer also makes the <code>kvzalloc()</code> failure path in <code>mlx5e_hv_vhca_stats_create()</code> reachable for the first time: it returns early without (re)creating the agent. Clear <code>priv->stats_agent.{agent,buf}</code> in <code>mlx5e_hv_vhca_stats_destroy()</code> after freeing them, so that if a later <code>create()</code> bails out on this path, a subsequent teardown does not double-free the stale agent/buffer left from a previous enable/disable cycle. This mirrors the existing <code>mlx5e</code> pattern of preallocating arrays of size <code>max_nch</code> (e.g. <code>priv->channel_stats</code>) and lazily populating entries up to <code>stats_nch</code> on demand.	2026-08-15	8.4	CVE-2026-72343
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>ntfs</code> : avoid stale runlist element dereference in <code>fallocate</code> <code>ntfs_attr_fallocate()</code> allocates holes and delayed allocations inside initialized size by looking up the current runlist element under <code>ni->runlist.lock</code> . The returned struct <code>runlist_element</code> is only a borrowed pointer into <code>ni->runlist.rl</code> . A writer can replace and free that array after the read lock is dropped, so later reads of <code>rl->lcn</code> , <code>rl->length</code> and <code>rl->vcn</code> can touch freed	2026-08-15	8.8	CVE-2026-72353

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory. The buggy scenario involves two paths, with each column showing the order within that path: ntfs_attr_fallocate(): 1. Take ni->runlist.lock for read. 2. Get rl from ntfs_attr_find_vcn_nolock(). 3. Drop ni->runlist.lock. 4. Read rl->lcn, rl->length and rl->vcn. mmap_page_mkwrite: 1. Enter ntfs_filemap_page_mkwrite(). 2. Reach __ntfs_write_iomap_begin() and ntfs_attr_map_cluster(). 3. Merge allocation state with ntfs_runlists_merge(). 4. Reallocate ni->runlist.ri in ntfs_ri_realloc(), freeing the old array. Validation reproduced this kernel report: BUG: KASAN: slab-use-after-free in ntfs_attr_fallocate+0xbb8/0xd00 Call Trace: <TASK> dump_stack_lvl+0x66/0xa0 print_report+0xce/0x630 ? ntfs_attr_fallocate+0xbb8/0xd00 ? srso_alias_return_thunk+0x5/0xfbef5 ? __virt_addr_valid+0x20d/0x410 ? ntfs_attr_fallocate+0xbb8/0xd00 kasan_report+0xe0/0x110 ? ntfs_attr_fallocate+0xbb8/0xd00 ntfs_attr_fallocate+0xbb8/0xd00 ? lock_acquire+0x2b8/0x2f0 ? __pfx_ntfs_attr_fallocate+0x10/0x10 ? 0xffffffff0000095 ? down_write+0x10d/0x1e0 ntfs_fallocate+0x5c9/0x1d00 ? __pfx_ntfs_fallocate+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 ? lock_acquire+0x2b8/0x2f0 ? srso_alias_return_thunk+0x5/0xfbef5 ? selinux_file_permission+0x3a7/0x510 vfs_fallocate+0x29d/0xd30 __x64_sys_fallocate+0xc7/0x150 ? do_syscall_64+0x81/0x6a0 do_syscall_64+0x115/0x6a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Allocated by task 410: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0xaa/0xb0 __kvmalloc_node_noprof+0x353/0x920 ntfs_ri_realloc+0x3f/0x110 ntfs_runlists_merge+0xaa3/0x3010 ntfs_attr_map_cluster+0x4e5/0xf80 ntfs_attr_fallocate+0x53f/0xd00 ntfs_fallocate+0x5c9/0x1d00 vfs_fallocate+0x29d/0xd30 __x64_sys_fallocate+0xc7/0x150 do_syscall_64+0x115/0x6a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 424: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 __kasan_slab_free+0x5f/0x80 kfree+0x307/0x580 ntfs_ri_realloc+0x6f/0x110 ntfs_runlists_merge+0x7b1/0x3010 ntfs_attr_map_cluster+0x4e5/0xf80 __ntfs_write_iomap_begin+0x8cd/0x2280 iomap_iter+0x6de/0x11e0 iomap_page_mkwrite+0x391/0x650 ntfs_filemap_page_mkwrite+0x1ac/0x400 do_page_mkwrite+0x15c/0x280 __handle_mm_fault+0xd6d/0x1ca0 handle_mm_fault+0x19c/0x470 do_user_addr_fault+0x23b/0x9c0 exc_page_fault+0x5c/0xc0 asm_exc_page_fault+0x26/0x30 Fix this by copying the needed runlist fields while the read lock is still held and using only those scalar snapshots after unlocking. After the snapshot, ntfs_attr_map_cluster() can also find that the range is already mapped and return balloc=false. Only call ntfs_dio_zero_range() when new clusters were allocated, matching the write iomap path and preserving the zero-newly-allocated-holes behavior.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: avoid stale runlist element dereference in MFT writeback ntfs_write_mft_block() maps each \$MFT record through the \$MFT data runlist. For sub-folio clusters it looks up a struct runlist_element under ni->runlist.lock, drops the lock, and later uses rl->length and rl->vcn when choosing folio_sz. That pointer is only borrowed from ni->runlist.ri. Concurrent \$MFT allocation extension can merge a replacement runlist under the same lock, and ntfs_ri_realloc() can free the old backing array. If that happens between the lookup and the later folio_sz decision, writeback can dereference freed runlist storage. The buggy scenario involves two paths, with each column showing the order within that path: MFT writeback path: \$MFT allocation extension: 1. Look up rl under 1. Extend the \$MFT data allocation. ni->runlist.lock. 2. Publish a replacement runlist. 2. Drop ni->runlist.lock. 3. Free the old runlist array. 3. Read rl->length and rl->vcn to choose folio_sz. Compute the remaining run length while ni->runlist.lock is still held, and use that scalar after unlock. This preserves the existing folio sizing decision without carrying a borrowed runlist_element across the lock boundary. Validation reproduced this kernel report: BUG: KASAN: slab-use-after-free in ntfs_mft_writepages+0x1c8d/0x1fb0 Call Trace: <TASK> dump_stack_lvl+0x66/0xa0 print_report+0xce/0x630 ? ntfs_mft_writepages+0x1c8d/0x1fb0 ? srso_alias_return_thunk+0x5/0xfbef5 ? __virt_addr_valid+0x20d/0x410 ? ntfs_mft_writepages+0x1c8d/0x1fb0 kasan_report+0xe0/0x110 ? ntfs_mft_writepages+0x1c8d/0x1fb0 ntfs_mft_writepages+0x1c8d/0x1fb0 ? __pfx_ntfs_mft_writepages+0x10/0x10 ? __pfx__mutex_unlock_slowpath+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 ? iput+0x92/0xa80	2026-08-15	8.8	CVE-2026-72354

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	do_writepages+0x219/0x530 ? __pfx_do_writepages+0x10/0x10 __writeback_single_inode+0x117/0xf50 ? do_raw_spin_lock+0x130/0x270 ? __pfx_do_raw_spin_lock+0x10/0x10 ? __pfx__writeback_single_inode+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 writeback_sb_inodes+0x65b/0x1810 ? srso_alias_return_thunk+0x5/0xfbef5 ? lock_acquire+0x2b8/0x2f0 ? __pfx_writeback_sb_inodes+0x10/0x10 ? lock_release+0x1e0/0x280 ? __raw_spin_unlock+0x23/0x40 ? move_expired_inodes+0x2b8/0x850 __writeback_inodes_wb+0xf4/0x270 ? __pfx__writeback_inodes_wb+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 ? queue_io+0x2e4/0x410 wb_writeback+0x666/0x880 ? srso_alias_return_thunk+0x5/0xfbef5 ? __pfx_wb_writeback+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 ? srso_alias_return_thunk+0x5/0xfbef5 ? get_nr_dirty_inodes+0x1c/0x170 wb_workfn+0x75e/0xbb0 ? srso_alias_return_thunk+0x5/0xfbef5 ? __raw_spin_unlock_irqrestore+0x27/0x60 ? __pfx_wb_workfn+0x10/0x10 ? __pfx_debug_object_deactivate+0x10/0x10 ? lock_acquire+0x2b8/0x2f0 ? srso_alias_return_thunk+0x5/0xfbef5 ? lock_release+0x1e0/0x280 process_one_work+0x8d0/0x1870 ? __pfx_process_one_work+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 worker_thread+0x575/0xf80 ? __pfx_worker_thread+0x10/0x10 kthread+0x2e7/0x3c0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x576/0x810 ? __pfx_ret_from_fork+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 ? __switch_to+0x57e/0xe10 ? __switch_to_asm+0x33/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> Allocated by task 970: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0xaa/0xb0 __kvmalloc_node_noprof+0x353/0x920 ntfs_rl_realloc+0x3c/0x80 ntfs_runlists_merge+0x1212/0x3010 ntfs_mft_data_extend_allocation_nolock+0x3e0/0x1f40 ntfs_mft_record_alloc+0x1ab4/0x4f10 __ntfs_create+0x680/0x2e50 ntfs_create+0x1e6/0x3a0 path_openat+0x2b55/0x3c10 do_file_open+0x1f4/0x460 do_sys_openat2+0xde/0x170 __x64_sys_openat+0x122/0x1e0 do_syscall_64+0x115/0x6a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 1294: kasan_save_---truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xen/pf: Don't attempt to process FAST_REQ or EVENT relays Currently defined VF/PF relay actions use regular REQUEST messages only and the PF shouldn't attempt to handle FAST_REQUEST nor EVENT messages as this would result in breaking the VFPF ABI protocol and also might trigger an assert on the PF side. (cherry picked from commit 1714d360fc5ae2e0886a69e979095d9c7ff3568a)	2026-08-15	8.4	CVE-2026-72360
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iomap: guard io_size EOF trim against concurrent truncate underflow iomap: fix zero padding data issue in concurrent append writes changed ioend accounting so that io_size tracks only valid data within EOF. This trims io_size when a writeback range extends past end_pos: ioend->io_size += map_len; if (ioend->io_offset + ioend->io_size > end_pos) ioend->io_size = end_pos - ioend->io_offset; However, if end_pos ends up below ioend->io_offset, the subtraction becomes negative and is stored in size_t io_size, causing an unsigned wrap to a huge value. This can happen when writeback continues past byte-level EOF up to a block-aligned range, or when a concurrent truncate shrinks the file after end_pos was sampled in iomap_writeback_handle_eof(). A wrapped io_size can mislead append detection and corrupt completion-time size handling, since filesystem end_io paths consume io_size for decisions such as on-disk EOF updates and unwritten/COW completion ranges. Fix this by clamping io_size to zero when EOF has moved to or before the ioend start offset. This preserves the original intent of trimming io_size to valid in-EOF data while avoiding the underflow.	2026-08-15	8.8	CVE-2026-72367
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xen/pvcalls: bound backend response req_id before indexing rsp[] pvcalls_front_event_handler() takes req_id directly from the backend-supplied ring response and uses it to index the fixed-size bedata->rsp[] array for a memcpy() and a store, with no range check. A malicious or buggy backend can set req_id past PVCALLS_NR_RSP_PER_RING and drive an out-of-bounds write past the bedata allocation. req_id was also declared int while the wire field rsp->req_id is u32, so a range check on the signed value alone is insufficient: a backend req_id of 0xffffffff becomes -1, passes a >= PVCALLS_NR_RSP_PER_RING test and indexes bedata->rsp[-1]. Declare req_id as u32 so a single bound covers both ends. A backend that	2026-08-15	8.8	CVE-2026-72380

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sends an out-of-range req_id has violated the wire protocol, so rather than silently dropping the response, log once and stop trusting the backend: set bedata->disabled. The event handler then ignores further responses, and the request paths that wait for a response return -EIO instead of blocking forever. This mirrors the fatal-error handling xen-netback uses (xenvif_fatal_tx_err()). The pvcalls frontend currently trusts its backend, so this is not a classic-Xen security issue, but it matters for hardening PV frontends against malicious backends (confidential and disaggregated deployments).			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: reject undersized DACLs before parsing ACEs parse_dacl() limits the attacker-controlled ACE count by comparing it with the number of minimal ACEs that fit in the DACL size. The DACL size field is 16 bits, but the expression subtracts sizeof(struct smb_acl). Because sizeof() is unsigned, a DACL size smaller than the ACL header underflows to a large size_t. A malicious client can reach this with: SMB2_SET_INFO (InfoType=SMB2_O_INFO_SECURITY) -> smb2_set_info_sec() -> set_info_sec() -> parse_sec_desc() -> parse_dacl() -> init_acl_state(..., 0xffff) -> init_acl_state(..., 0xffff) -> kcalloc_objs(..., 0xffff) Thus a malformed security descriptor can make num_aces pass the guard and drive large temporary ACL state and pointer-array allocations. Reject DACLs smaller than struct smb_acl before doing the subtraction, so the ACE count check cannot be bypassed by the underflow.	2026-08-15	8.8	CVE-2026-72382
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: md/raid5: avoid R5_Overlap races while breaking stripe batches KCSAN report a race in break_stripe_batch_list() vs. raid5_make_request() on sh->dev[i].flags (plain word write vs. atomic bit op).. and .. one possible scenario is: CPU1 CPU2 break_stripe_batch_list(sh1) -> handle sh2 -> lock(sh2) -> sh2->batch_head = NULL -> unlock(sh2) -> test_and_clear_bit(R5_Overlap, sh2->dev[i].flags) -> wake_up_bit(sh2->dev[i].flags) raid5_make_request() -> add_all_stripe_bios(sh2) -> lock(sh2) -> stripe_bio_overlaps(sh2) returns true batch_head is NULL, so new bio overlap exist bio on sh2 -> true -> set_bit(R5_Overlap, sh2->dev[i].flags) -> unlock(sh2) -> wait_on_bit(sh2->dev[i].flags) -> sh2->dev[i].flags = sh1->dev[i].flags & ~R5_Overlap No wait_up_bit(), CPU2 could be wait_on_bit() forever... Fix by : - Expand the protect zone. - Use batch_head's device flag's snapshot when no held head_sh->stripe_lock. - Move sh/head_sh->batch_head = NULL to the end of protected zone , and , any concurrent add_all_stripe_bios() grabs sh->stripe_lock now either: - see batch_head != null, and , is rejected by stripe_bio_overlaps() under the lock (no R5_Overlap wait) , or , - sees batch_head == NULL, only after dev[i].flags has already been set and the prior R5_Overlap waiters worken. KCSAN report: ===== BUG: KCSAN: data-race in break_stripe_batch_list / raid5_make_request write (marked) to 0xffff8e89c8117548 of 8 bytes by task 4042 on cpu 0: raid5_make_request+0xea0/0x2930 md_handle_request+0x4a2/0xa40 md_submit_bio+0x109/0x1a0 __submit_bio+0x2ec/0x390 submit_bio_noacct_nocheck+0x457/0x710 submit_bio_noacct+0x2a7/0xc20 submit_bio+0x56/0x250 blkdev_direct_IO+0x54c/0xda0 blkdev_write_iter+0x38f/0x570 aio_write+0x22b/0x490 io_submit_one+0xa51/0xf70 __x64_sys_io_submit+0xf7/0x220 x64_sys_call+0x1907/0x1c60 do_syscall_64+0x130/0x570 entry_SYSCALL_64_after_hwframe+0x76/0x7e read to 0xffff8e89c8117548 of 8 bytes by task 4010 on cpu 5: break_stripe_batch_list+0x249/0x480 handle_stripe_clean_event+0x720/0x9b0 handle_stripe+0x32fb/0x4500 handle_active_stripes.isra.0+0x6e0/0xa50 raid5d+0x7e0/0xba0 md_thread+0x15a/0x2d0 kthread+0x1e3/0x220 ret_from_fork+0x37a/0x410 ret_from_fork_asm+0x1a/0x30 value changed: 0x0000000000000019 -> 0x0000000000000099 --> R5_Overlap	2026-08-15	8.8	CVE-2026-72420
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Guard conntrack opts error writes The conntrack lookup and allocation kfuncs take an opts pointer together with an opts__sz argument. The verifier checks only the memory range described by opts__sz, but the wrappers unconditionally write opts->error whenever the internal lookup or allocation helper returns an error. For an invalid size smaller than the end of opts->error, that write can land outside the verifier-checked range. Keep returning NULL for invalid arguments, but only report the error through opts->error when the supplied size includes the field. This preserves error reporting for the supported 12-byte and 16-byte layouts, and for other invalid sizes that still include opts->error.	2026-08-15	8.8	CVE-2026-72423

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Preserve pointer spill metadata during half-slot cleanup __clean_func_state() cleans dead stack slots in 4-byte halves. When the high half of a STACK_SPILL slot is dead and the low half remains live, cleanup converts the live low half to STACK_MISC or STACK_ZERO and clears the saved spilled_ptr metadata. That conversion is safe only for scalar spills. For a pointer spill, this metadata clear lets a later 32-bit fill from the still-live half avoid the normal non-scalar register-fill check and be treated as an ordinary scalar stack read. Leave non-scalar spill slots intact in this half-live shape. This is conservative for pruning and preserves the existing check_stack_read_fixed_off() rejection path for partial fills from pointer spills.	2026-08-15	8.4	CVE-2026-72426
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix race in unix socket mediation when peer_path is used The holding a reference to the peer_sk is not enough to ensure access to the peer sk path. Accessing the path outside of the state lock allows for a race with unix_release_sock(). Fix this by taking the state lock and getting a reference to the path under lock. Ideally for connected sockets we would cache this information so we don't have to take the lock here. But for now just fix the race.	2026-08-15	8.8	CVE-2026-72462
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xprtrdma: Fix ep kref imbalance on ADDR_CHANGE rprcdma_cm_event_handler() falls through to the disconnected: label on RDMA_CM_EVENT_ADDR_CHANGE and calls rprcdma_ep_put() with no matching get when the event arrives before RDMA_CM_EVENT_ESTABLISHED. The kref then underflows during connect teardown and rprcdma_xprt_disconnect() operates on a freed ep. Reference counts across a normal connection lifecycle: rprcdma_ep_create() kref_init ->1 rprcdma_xprt_connect() ep_get ->2 (before post_recvs) RDMA_CM_EVENT_ESTABLISHED ep_get ->3 RDMA_CM_EVENT_DISCONNECTED ep_put ->2 rprcdma_xprt_drain() ep_put ->1 rprcdma_xprt_disconnect() tail ep_put ->0 (ep_destroy) The connect-time get in rprcdma_xprt_connect(), taken just before rprcdma_post_recvs() "while there are outstanding Receives," is balanced by rprcdma_xprt_drain. ADDR_CHANGE before ESTABLISHED has no get to consume, so its put drops the count to 1 and the drain put then frees the ep while rprcdma_xprt_disconnect() still holds a pointer to it. Fix by dispatching on the prior re_connect_status via xchg(): for prev == 0 (pre-ESTABLISHED) wake the connect waiter and return with no put; for prev == 1 call rprcdma_force_disconnect() and return. The case-1 arm relies on the subsequent RDMA_CM_EVENT_DISCONNECTED event -- reliably delivered when rdma_disconnect() is called on a still-connected cm_id -- to balance the ESTABLISHED get; rprcdma_xprt_drain() continues to balance only that connect-time get. Any other prior value means teardown is already in flight.	2026-08-15	8.8	CVE-2026-72469
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: add bounds check to run_get_highest_vcn() run_get_highest_vcn() parses a packed NTFS mapping-pairs buffer without any length bound, relying solely on a 0x00 terminator to stop. A crafted \$LogFile UpdateMappingPairs record whose embedded attribute contains mapping-pairs runs without a terminator causes the function to read past the slab allocation, triggering a KASAN slab-out-of-bounds read on mount. The sibling function run_unpack() received an analogous bounds-check in commit b62567bca474 ("ntfs3: add buffer boundary checks to run_unpack()"), but run_get_highest_vcn() was missed. Take a run_buf_size parameter and reject any run header whose payload would extend past the buffer end, mirroring the pattern used by run_unpack(). The caller in fslog.c passes the remaining attribute bytes after the mapping-pairs offset. KASAN report (on mainline v7.1 merge window HEAD): BUG: KASAN: slab-out-of-bounds in run_get_highest_vcn+0x3c0/0x410 Read of size 1 at addr ffff88800e2d5400 by task mount/72 Call Trace: run_get_highest_vcn+0x3c0/0x410 do_action.isra.0+0x3ba8/0x7b50 log_replay+0x9ddd/0x10200 ntfs_loadlog_and_replay+0x4ad/0x610 ntfs_fill_super+0x214a/0x4540	2026-08-15	8.4	CVE-2026-72478
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: staging: nvec: fix use-after-free in nvec_rx_completed() In nvec_rx_completed(), when an incomplete RX transfer is detected, nvec_msg_free() is called to return the message back to the pool by clearing its 'used' atomic flag. Immediately after this, the code accesses nvec->rx->data[0] to check the message type. Since nvec_msg_free() marks the pool slot as available via atomic_set(), any concurrent or subsequent call to nvec_msg_alloc() could claim that same slot and overwrite its data[] array. Reading nvec->rx->data[0] after freeing the message is therefore a	2026-08-15	8.4	CVE-2026-72489

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	use-after-free. Fix this by saving the message type byte before calling nvec_msg_free(), then using the saved value for the battery quirk check.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in same_client_has_lease() same_client_has_lease() returns an opinfo pointer from ci->m_op_list after dropping ci->m_lock without taking a reference. smb_grant_oplock() then dereferences that pointer in copy_lease() and when checking breaking_cnt. A concurrent close can remove the old lease from ci->m_op_list and drop the last reference before the caller uses the returned pointer, leading to a use-after-free. Take a reference when same_client_has_lease() selects an existing lease, drop any previous match while scanning, and release the returned reference in smb_grant_oplock() after copying the lease state.	2026-08-15	8.8	CVE-2026-72492
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Add a max slot check for SQ. The variable WQE mode must be validated against the maximum slots supported by HW. The max supported value is 64K. Adding a max and min check and fail if user supplied value is more than the max supported and zero.	2026-08-15	8.8	CVE-2026-72497
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Free CQ toggle page after firmware teardown Free the toggle page only after firmware teardown completes so that an NQ interrupt arriving during bnxt_qplib_destroy_cq() won't write the toggle value to an already-freed page. Move free_page() after bnxt_qplib_destroy_cq.	2026-08-15	8.8	CVE-2026-72499
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Free SRQ toggle page after firmware teardown Free the toggle page only after firmware teardown completes so that an NQ interrupt arriving during bnxt_qplib_destroy_srql() won't write the toggle values to an already-freed page. Move free_page() after bnxt_qplib_destroy_srql().	2026-08-15	8.8	CVE-2026-72500
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf, sockmap: fix integer overflow in bpf_msg_pop_data() bounds check start and len are u32, so u64 last = start + len; evaluates start + len in 32-bit and wraps before storing it in last. The bounds check if (start >= offset + l last > msg->sg.size) return -EINVAL; can then be passed with an out-of-range start/len, after which the pop loop runs off the end of the scatterlist and sk_msg_shift_left() calls put_page() on the empty msg->sg.end slot: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000001: 0000 [#1] SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000008-0x000000000000000f] RIP: 0010:sk_msg_shift_left net/core/filter.c:2957 [inline] RIP: 0010:___bpf_msg_pop_data net/core/filter.c:3103 [inline] RIP: 0010:bpf_msg_pop_data+0x753/0x1a10 net/core/filter.c:2984 Call Trace: <TASK> bpf_prog_4cc92c278f4d5d56+0x1b1/0x1e8 bpf_prog_run_pin_on_cpu+0x107/0x320 include/linux/filter.h:746 sk_psock_msg_verdict+0x357/0x7f0 net/core/skmsg.c:934 tcp_bpf_send_verdict net/ipv4/tcp_bpf.c:420 [inline] tcp_bpf_sendmsg+0x766/0x1ae0 net/ipv4/tcp_bpf.c:583 __sock_sendmsg+0x153/0x1c0 net/socket.c:802 __sys_sendto+0x326/0x430 net/socket.c:2265 __x64_sys_sendto+0xe3/0x100 net/socket.c:2268 do_syscall_64+0x14c/0x480 entry_SYSCALL_64_after_hwframe+0x77/0x7f </TASK> Widen the addition with a (u64) cast so the bound is evaluated in 64-bit and a len near U32_MAX no longer wraps below msg->sg.size. While here, change pop from int to u32. It counts bytes against the unsigned scatterlist lengths and can never be negative, so the signed type only invites sign-confusion in the pop loop.	2026-08-15	8.4	CVE-2026-74256
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: cifs: remove all cifs files before kill super Cifs files may be put into fileinfo_put_wq during umounting cifs. After umount done, cifsFileInfo_put_final is called, which cause following BUG: BUG: kernel NULL pointer dereference, address: 0000000000000000 ... [134.222152] list_lru_add+0x64/0x1a0 [134.222399] ? cifs_put_tcon+0x171/0x340 [cifs] [134.222772] d_lru_add+0x44/0x60 [134.222997] dput+0x1fc/0x210 [134.223213] cifsFileInfo_put_final+0x11a/0x140 [cifs] [134.223576] process_one_work+0x17c/0x320 [134.223843] worker_thread+0x188/0x280 [134.224084] ? __pfx_worker_thread+0x10/0x10 [134.224366] kthread+0xcc/0x100 [134.224576] ? __pfx_kthread+0x10/0x10 [134.224827] ret_from_fork+0x30/0x50 [134.225063] ? __pfx_kthread+0x10/0x10 [134.225328] ret_from_fork_asm+0x1b/0x30 This can be reproduce by following: unshare -n bash -c " mkdir -p \${CIFS_MNT} ip netns attach root 1 ip link add eth0 type veth peer veth0 netns root ip link set eth0 up -n root link set veth0 up ip	2026-08-15	8.4	CVE-2026-74259

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	addr add 192.168.0.2/24 dev eth0 ip -n root addr add 192.168.0.1/24 dev veth0 ip route add default via 192.168.0.1 dev eth0 ip netns exec root sysctl net.ipv4.ip_forward=1 ip netns exec root iptables -t nat -A POSTROUTING -s 192.168.0.2 -o \${DEV} -j MASQUERADE mount -t cifs \${CIFS_PATH} \${CIFS_MNT} -o vers=3.0,sec=ntlmssp,credentials=\${CIFS_CRED},rsize=65536,wsiz=65536,cache=none,echo_interval=1 touch \${CIFS_MNT}/a.txt ip netns exec root iptables -t nat -D POSTROUTING -s 192.168.0.2 -o \${DEV} -j MASQUERADE " umount \${CIFS_MNT}			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: cxl/region: Fix out-of-bounds access in cxl_cancel_auto_attach() In cxl_cancel_auto_attach(), it assumes cxled->pos is a valid index for accessing p->targets[]. However, cxled->pos can be set to negative errno in cxl_region_sort_targets() if cxl_calc_interleave_pos() fails. This causes the driver to use a negative index to access p->targets[], resulting in out-of-bounds access. Fix it by walking p->targets[] instead of using cxled->pos directly.	2026-08-15	8.4	CVE-2026-74275
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/dma-iommu: Fix wrong scatterlist length assignment in P2PDMA path In iommu_dma_map_sg(), when handling PCI P2PDMA cases, the DMA length of the current scatterlist segment `s` is incorrectly assigned from the head entry `sg->length` instead of the current entry `s->length`. This typo causes all P2PDMA segments in the scatterlist to inherit the length of the first segment, leading to corrupted DMA lengths for multi- segment scatterlists. Fix this by using `s->length` instead of `sg->length`.	2026-08-15	8.8	CVE-2026-74277
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: Stop leased rxq before uninstalling its memory provider netif_rxq_cleanup_unlease() tears down the memory provider that was installed on a physical RX queue through a netkit queue lease. It currently revokes the provider's DMA mappings before stopping the physical queue: __netif_mp_uninstall_rxq(virt_rxq, p); /* DMA unmap */ __netif_mp_close_rxq(phys_rxq->dev, rxq_idx, p); /* queue stop */ This inverts the ordering used by the regular teardown paths (normal device unregister and the io_uring zcrx close path), which stop the queue before revoking the provider's mappings. With the physical queue still live, its NAPI can keep consuming net_iov entries from the page_pool alloc cache after the __netif_mp_uninstall_rxq() has already cleared their dma_addr, opening a window for the device to DMA to a stale or zero address. Fix it by swapping the two calls so the queue is stopped (and its NAPI quiesced) before the provider is uninstalled. No functional regression was observed across repeated runs of the nk_qlease.py HW selftest, which exercises the lease teardown path; this was tested against fbnci QEMU emulation.	2026-08-15	8.8	CVE-2026-74285
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci: validate codec capability element length Read Local Codec Capabilities returns a sequence of capability elements. Each element starts with a one-byte length followed by that many payload bytes. hci_read_codec_capabilities() checks that the skb contains the length byte, but then validates only caps->len against the remaining skb length. A malformed controller response with one remaining byte and caps->len set to one passes that check even though the element needs two bytes. The parser then records a two-byte capability and copies one byte beyond the advertised response payload into the codec list. Validate the full element size, including the length byte, before adding it to the accumulated capability length. This preserves all well-formed capability elements and drops only truncated controller responses.	2026-08-15	8.8	CVE-2026-74300
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vduse: hold vduse_lock across IDR lookup in open path vduse_dev_open() looks up struct vduse_dev through the IDR and then acquires dev->lock only after vduse_lock has been dropped. This leaves a window where a concurrent VDUSE_DESTROY_DEV can remove the same object from the IDR and free it before the open path locks the device, leading to a use-after-free. Close this race by keeping vduse_lock held until dev->lock has been acquired in the open path, matching the lock ordering already used by the destroy path.	2026-08-15	8.8	CVE-2026-74313
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7996: Fix possible token leak in mt7996_tx_prepare_skb() If link_conf or link_sta lookup fails in mt7996_tx_prepare_skb routine, mt7996 driver leaks an already allocated tx token. Fix the issue releasing the token in case of error.	2026-08-15	8.8	CVE-2026-74323
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommufd: Destroy the pages content after detaching from dmabuf Sashiko points out this has gotten out of order, the mutex could still be in use through the dmabuf invalidation	2026-08-15	8.8	CVE-2026-74328

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	callbacks. Don't destroy any of the pages content until the dmabuf is fully detached.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp-sdw-sof: Bound DAI link iteration create_sdw_dailinks() walks sof_dais until it finds an entry with initialised cleared, but sof_dais is allocated with exactly num_ends entries. If all entries are initialised, the loop reads past the end of the array. Pass the allocated entry count to create_sdw_dailinks() and stop before reading past the array.	2026-08-15	8.4	CVE-2026-74332
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp-sdw-legacy: Bound DAI link iteration create_sdw_dailinks() walks soc_dais until it finds an entry with initialised cleared, but soc_dais is allocated with exactly num_ends entries. If all entries are initialised, the loop reads past the end of the array. This was reported by KASAN: BUG: KASAN: slab-out-of-bounds in mc_probe+0x26b3/0x2774 [snd_acp_sdw_legacy_mach] Read of size 1 Pass the allocated entry count to create_sdw_dailinks() and stop before reading past the array.	2026-08-15	8.4	CVE-2026-74333
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: wcn36xx: fix OOB read from firmware count in PRINT_REG_INFO indication The firmware-controlled rsp->count field is used as the loop bound for indexing into the flexible rsp->regs[] array without validation against the message length. A count exceeding the actual data causes out-of- bounds reads from the heap-allocated message buffer. Add a check that count fits within the received message.	2026-08-15	8.1	CVE-2026-74340
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: wcn36xx: fix heap overflow from oversized firmware HAL response The firmware response dispatcher copies all synchronous HAL responses into the 4096-byte hal_buf without validating the response length. A response exceeding WCN36XX_HAL_BUF_SIZE causes a heap buffer overflow with firmware-controlled content. Add a bounds check on the response length.	2026-08-15	8.8	CVE-2026-74341
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Fix RB-tree corruption in probe error path The info->node RB-tree member is zero-initialized via kzalloc. If a device does not support ATS, the device_rbtrees_insert() call is skipped. If a subsequent probe step fails, the error path jumps to device_rbtrees_remove(), which misinterprets the zeroed node as a tree root and corrupts the device RB-tree. Fix this by explicitly initializing the RB-node as empty using RB_CLEAR_NODE() during initialization and guarding the removal with RB_EMPTY_NODE().	2026-08-15	8.2	CVE-2026-74355
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gpu: host1x: Fix iommu_map_sgtable() return value check Commit "iommu: return full error code from iommu_map_sg_atomic()" changed iommu_map_sgtable() to return an ssize_t and negative values in error cases, rather than a size_t and a zero. pin_job() also was incorrectly assigning to 'int', which could cause overflows into negative values. Update pin_job() to correctly check for errors from iommu_map_sgtable.	2026-08-15	8.8	CVE-2026-74380
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvme-pci: fix out-of-bounds access in nvme_setup_descriptor_pools nvme_setup_descriptor_pools() indexes dev->descriptor_pools[] using the numa_node forwarded from hctx->numa_node by its single caller, nvme_init_hctx_common(). On a non-NUMA kernel hctx->numa_node is NUMA_NO_NODE (-1). Because the parameter was declared 'unsigned', the value becomes UINT_MAX and the index walks off the array (sized to nr_node_ids), faulting during nvme_alloc_ns() and leaving the namespace without a /dev node. Reproduces on any NVMe controller probed by a CONFIG_NUMA=n kernel: BUG: unable to handle page fault for address: ffff889101603d38 RIP: 0010:nvme_init_hctx_common+0x5a/0x190 [nvme] Call Trace: nvme_init_hctx+0x10/0x20 [nvme] nvme_alloc_ns+0x9e/0xa10 [nvme_core] nvme_scan_ns+0x301/0x3b0 [nvme_core] nvme_scan_ns_async+0x23/0x30 [nvme_core] Switch the parameter to int and fall back to node 0 when it is NUMA_NO_NODE; node 0 is always present.	2026-08-15	8.4	CVE-2026-74383
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: cancel SSR work items during PCI shutdown A reboot can crash the kernel if it overlaps with WLAN firmware crash recovery (SSR). The crash is a NULL pointer dereference in the MHI teardown path while freeing DMA-backed MHI contexts. Simplified trace: dma_free_attrs mhi_deinit_dev_ctxt [mhi] ath11k_pci_power_down [ath11k_pci] ath11k_pci_shutdown [ath11k_pci] device_shutdown kernel_restart On the host side, SSR is driven by the MHI RDDM callback, which queues reset_work to perform device recovery. reset_work power-	2026-08-15	8.8	CVE-2026-74407

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cycles the device by calling ath11k_hif_power_down() followed by ath11k_hif_power_up(). The power-down phase deinitializes MHI and frees DMA resources. Shutdown/reboot runs fully asynchronously with this RDDM-driven SSR recovery flow. As a result, the shutdown path (ath11k_pci_shutdown() -> ath11k_pci_power_down()) can race with the SSR recovery sequence. Fix this by canceling SSR-related work items during PCI shutdown, marking the device as unregistering, and serializing the RDDM callback path that checks and queues reset_work. This ensures that no new SSR recovery work can be queued once teardown has started, and that any in-flight recovery work is fully synchronized before device power-down, preventing MHI teardown and DMA resource freeing from running more than once. Note: This issue only affects PCI/MHI-based devices. AHB-based ath11k devices do not queue reset_work in normal SSR flows. Tested-on: WCN6855 hw2.1 PCI WLAN.HSP.1.1-04866.5-QCAHSPSWPL_V1_V2_SILICONZ_IOE-1			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath9k: fix OOB access from firmware tx status queue ID ath_tx_edma_tasklet() accesses sc->tx.txq[ts.qid] where ts.qid is a 4-bit hardware field (0-15), but the txq array only has ATH9K_NUM_TX_QUEUES (10) entries. A qid >= 10 causes an OOB array access. Add a bounds check on ts.qid before using it as an array index.	2026-08-15	8.8	CVE-2026-74408
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: add bounds check on firmware mac_id in link lookup The mac_id field in RX descriptors is 8 bits wide (0-255), but assoc_link_on_macid[] has only RTW89_MAX_MAC_ID_NUM (128) entries. While the driver currently assigns mac_id values below 128, the descriptor value comes from firmware and is not validated before use as an array index. Add a defensive bounds check in rtw89_assoc_link_rcu_dereference() to guard against out-of-range firmware values.	2026-08-15	8.8	CVE-2026-74409
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: fix OOB read from firmware RX descriptor exceeding DMA buffer In rtw_pci_rx_napi(), new_len is computed as the sum of pkt_len (14-bit descriptor field, max 16383) and pkt_offset (drv_info_sz + shift, both firmware-controlled). The result can exceed RTK_PCI_RX_BUF_SIZE (11478), causing an out-of-bounds read from the pre-allocated DMA buffer when skb_put_data copies new_len bytes. The USB transport already validates this (rtw_usb_rx_data_put checks against RTW_USB_MAX_RECVBUF_SZ); the PCIe path does not. Add a check that new_len does not exceed the DMA buffer size.	2026-08-15	8.1	CVE-2026-74410
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: Correct data type for scan index to avoid infinite loop A kernel soft lockup was observed during Wi-Fi scanning on the 6GHz band. The CPU becomes stuck in rtw89_hw_scan_add_chan_ax for over 20 seconds, leading to a system panic. RIP points to 0f b6 c3 (movzbl %bl, %eax), which zero-extends the low 8 bits of RBX into RAX. RBX (the counter i) has reached a huge value: 0x137466a1. watchdog: BUG: soft lockup - CPU#2 stuck for 26s! [kworker/u16:4:6124] Workqueue: events_unbound cfg80211_wiphy_work [cfg80211] RIP: 0010:rtw89_hw_scan_add_chan_ax+0xb3/0xe0 [rtw89_core] Code: a0 48 89 45 a8 44 89 6d 9c 44 89 75 98 eb 29 66 66 2e 0f 1f 84 00 00 00 00 00 66 66 2e 0f 1f 84 00 00 00 00 00 66 90 83 c3 01 <0f> b6 c3 41 3b 44 24 74 0f 83 0b 02 00 00 0f b6 c3 48 8d 14 80 49 RSP: 0018:ffffcb48cbaa39f8 EFLAGS: 00000202 RAX: 0000000000000005 RBX: 000000000137466a1 RCX: 0000000000000000 RDX: ffff89ffc9d851a8 RSI: 00000000000004f0d RDI: 0000000096af0130 RBP: ffffcb48cbaa3a60 R08: 0000000000000000 R09: ffff8a00b7502080 R10: ffff8a00b75ff600 R11: 0000000000000000 R12: ffff89ffc7553870 R13: ffff8a00b7ac8f19 R14: ffff8a00b75020d8 R15: ffff89ffc3d54d80 FS: 0000000000000000(0000) GS:ffff8a014f962000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007558d7f9f4c4 CR3: 0000000178040001 CR4: 00000000001706f0 Call Trace: <TASK> rtw89_hw_scan_prep_chan_list_ax+0x8a/0x400 [rtw89_core] rtw89_hw_scan_start+0x546/0x8a0 [rtw89_core] ? rtw89_fw_h2c_default_cmac_tbl+0x13c/0x1f0 [rtw89_core] rtw89_ops_hw_scan+0xae/0x120 [rtw89_core] drv_hw_scan+0xbb/0x180 [mac80211] __ieee80211_start_scan+0x2fc/0x750 [mac80211] ieee80211_request_scan+0xe/0x20 [mac80211] ieee80211_scan+0x123/0x190 [mac80211] rdev_scan+0x40/0x110 [cfg80211] cfg80211_scan_6ghz+0x5a1/0xa30 [cfg80211] By objdump with source: for (i = 0; i < req->n_6ghz_params; i++) { 5fbc0: 83 c3 01 add \$0x1,%ebx --> i++ 5fbc3: 0f b6 c3 movzbl %bl,%eax --> get	2026-08-15	8.8	CVE-2026-74411

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	counter fbc6: 41 3b 44 24 74 cmp 0x74(%r12),%eax * RBX: 00000000137466a1 -> %bl = a1 -> EAX = 000000a1 (161)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: fix wrong pci_get_drvdata type in AER handlers rtw88 stores an ieee80211_hw pointer via pci_set_drvdata() at probe time, but io_error_detected() and io_resume() retrieve it as a net_device pointer. This causes netif_device_detach/attach to operate on an ieee80211_hw struct, reading and writing at wrong offsets. Use ieee80211_stop_queues/wake_queues instead, consistent with every other queue stop/start path in the driver.	2026-08-15	8.8	CVE-2026-74412
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: fix wrong pci_get_drvdata type in AER handlers rtw89 stores an ieee80211_hw pointer via pci_set_drvdata() at probe time, but io_error_detected() and io_resume() retrieve it as a net_device pointer. This causes netif_device_detach/attach to operate on an ieee80211_hw struct, reading and writing at wrong offsets. The adjacent io_slot_reset() already does it correctly. Use ieee80211_stop_queues/wake_queues instead, consistent with every other queue stop/start path in the driver. Tested on RTL8852CE by calling the handlers from a test module before and after the fix.	2026-08-15	8.8	CVE-2026-74413
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: bound DMA command body size against suffix pointer vmw_cmd_dma() locates the DMA suffix at (unsigned long) &cmd->body + header->size - sizeof(*suffix) without checking that header->size is large enough to contain both cmd->body and the suffix. An undersized header makes the suffix pointer underflow back into the previous command in the bounce buffer. The verifier later writes suffix->maximumOffset, clobbering verified fields of an already-relocated earlier command -- a TOCTOU on the device-visible command stream that lets one command rewrite another's GMR id, surface id, or other authenticated fields. Reject the command if the body is too small for the suffix to fit.	2026-08-15	8.8	CVE-2026-74443
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: i2c: imx: Cancel hrtimer before clearing slave pointer In i2c_imx_unreg_slave(), the slave pointer is set to NULL after disabling interrupts. However, a pending interrupt might already have started the hrtimer (i2c_imx_slave_timeout) before the pointer was cleared. If the hrtimer fires after i2c_imx->slave is set to NULL, the timer callback i2c_imx_slave_finish_op() will call i2c_imx_slave_event() with a NULL slave pointer, which results in a use-after-free / NULL pointer dereference. Fix by canceling the hrtimer and waiting for it to complete after disabling interrupts, before clearing the slave pointer.	2026-08-15	8.4	CVE-2026-74461
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: prevent peer transport count overflow sctp_assoc_add_peer() increments the association's 16-bit transport_count for every new unique peer. Adding the 65,536th transport wraps the count to zero. SCTP sock_diag uses transport_count to reserve the INET_DIAG_PEERS payload, then copies one sockaddr_storage for every entry in transport_addr_list. After the wrap, a diagnostic dump reserves an empty payload and writes 8 MiB of peer addresses past the skb tail. Reject a new unique peer when transport_count has reached U16_MAX. Perform the check after the existing-peer lookup so a duplicate address continues to return its existing transport at the limit.	2026-08-15	8.8	CVE-2026-74469
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: use the subframe length when parsing A-MSDU TDLS frames mwifiex_11n_dispatch_amsdu_pkt() splits an A-MSDU with ieee80211_amsdu_to_8023s() and walks the resulting subframes. For each subframe it passes the subframe data pointer to mwifiex_process_tlds_action_frame(), but pairs it with skb->len, the length of the A-MSDU parent, instead of rx_skb->len: rx_skb = __skb_dequeue(&list); rx_hdr = (struct rx_packet_hdr *)rx_skb->data; if (ISSUPP_TDLS_ENABLED(priv->adapter->fw_cap_info) && ntohs(rx_hdr->eth803_hdr.h_proto) == ETH_P_TDLS) { mwifiex_process_tlds_action_frame(priv, (u8 *)rx_hdr, skb->len); } The parent is not a valid description of that buffer, and may not be valid memory at all. ieee80211_amsdu_to_8023s() ends with if (!reuse_skb) dev_kfree_skb(skb); and it only sets reuse_skb when the parent is linear, is not a head_frag, and is being consumed as the *last* subframe. So when the parent does not qualify for reuse it has already been freed, and the read of skb->len is a use-after-free. When it is reused, skb->len is the length of the last subframe, applied to every earlier subframe, which over-states the buffer whenever an earlier subframe is shorter.	2026-08-15	8.8	CVE-2026-74488

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The callee cannot absorb a wrong length, because it derives its own ceiling from the value it is given. Each frame type computes <code>ies_len = len - sizeof(struct ethhdr) - TDLS_*_FIX_LEN</code> ; and the element walk is then bounded entirely against that ceiling, for <code>(end = pos + ies_len; pos + 1 < end; pos += 2 + pos[1]) { u8 ie_len = pos[1]; if (pos + 2 + ie_len > end) break; so a too-large len moves end past the end of the subframe and the walk reads and copies beyond it. The A-MSDU layout is chosen by the sender, which makes the difference between the last subframe and a shorter earlier one remotely selectable. Reaching this requires TDLS support in firmware and the TDLS ethertype on the subframe. The other caller, <code>mwifiex_process_rx_packet()</code>, is correct: it passes a pointer and a length that describe the same region of the RX buffer. Pass <code>rx_skb->len</code>, the length of the subframe actually being parsed.</code>			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix <code>tid_tx</code> use-after-free on BA session stop <code>ieee80211_stop_tx_ba_cb()</code> hands <code>tid_tx</code> to <code>kfree_rcu()</code> through <code>ieee80211_remove_tid_tx()</code> , and then reads <code>tid_tx->ndp</code> after dropping <code>sta->lock</code> : <code>ieee80211_remove_tid_tx(sta, tid); /* kfree_rcu(tid_tx, rcu_head) */ ... spin_unlock_bh(&sta->lock); if (start_txq) ieee80211_agg_start_txq(sta, tid, false); if (send_delba) ieee80211_send_delba(..., tid_tx->ndp);</code> That read is not covered by an RCU read-side critical section, and it runs in preemptible process context: both callers hold the wiphy mutex, reaching it either from the <code>ieee80211_ba_session_work()</code> wiphy work or from <code>ieee80211_sta_tear_down_BA_sessions()</code> during station teardown. Softirqs can run in that window too, both from the <code>local_bh_enable()</code> that ends <code>ieee80211_agg_start_txq()</code> and from any interrupt exit, so the RCU callback can free <code>tid_tx</code> before the read. Driving the function from a test module with the grace period forced into that window, KASAN reports the read, and the free arrives on the ordinary RCU softirq path: BUG: KASAN: slab-use-after-free in <code>ieee80211_stop_tx_ba_cb+0x3cd/0x400</code> Read of size 1 at addr <code>ffff888002b9f52e</code> by task <code>kworker/0:1/10</code> [...] Freed by task 57: <code>__kasan_slab_free+0x47/0x70</code> <code>__rcu_free_sheaf_prepare+0x70/0x250</code> <code>rcu_free_sheaf_nobarn+0x18/0x40</code> <code>rcu_core+0x426/0x1310</code> <code>handle_softirqs+0x144/0x590</code> <code>__irq_exit_rcu+0xea/0x150</code> <code>irq_exit_rcu+0x9/0x20</code> <code>sysvec_apic_timer_interrupt+0x6b/0x80</code> <code>asm_sysvec_apic_timer_interrupt+0x1a/0x20</code> <code>send_delba</code> is only set when <code>tx_stop</code> is set, which happens for <code>AGG_STOP_LOCAL_REQUEST</code> alone, so this is reached on local teardown - session idle timeout, PTK rekey, suspend, HW reconfig - and not from a peer's DELBA. Read <code>ndp</code> into a local before the session is freed, while <code>sta->lock</code> is still held. <code>tid_tx->ndp</code> has a single writer, in <code>ieee80211_tx_ba_session_handle_start()</code> , which cannot run concurrently here: both paths are serialised by the wiphy mutex, and the session is already marked <code>HT_AGG_STATE_STOPPING</code> at this point. <code>tid_tx->ndp</code> is also the only <code>tid_tx</code> dereference left after <code>ieee80211_remove_tid_tx()</code> in this function. [move/change the comment a bit to be more general not just on <code>ndp</code> , initialize <code>ndp</code> directly]	2026-08-15	8.8	CVE-2026-74489
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: avoid use-after-free in poll trace queue dumps TIPC socket tracepoints dump queue state through <code>tipc_sk_dump()</code> . Most queue-dump callsites already serialize that walk under the socket lock or <code>sk->sk_lock.slock</code> , but <code>tipc_poll()</code> calls <code>trace_tipc_sk_poll(..., TIPC_DUMP_ALL, ...)</code> without holding either lock. That lets the poll trace path reach <code>tipc_list_dump()</code> and backlog head/tail dumping while another context dequeues and frees an <code>skb</code> , leaving the trace helper dereferencing a stale queue entry. Stop the unlocked poll trace site from requesting queue dumps. Other queue dump trace callsites keep their existing output under the locking they already provide, while poll still emits the event itself without walking live queue members from an unlocked context.	2026-08-15	8.8	CVE-2026-74490
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: do not update comments from kernel-side hash adds <code>mtype_resize()</code> copies comment pointers with <code>memcpy()</code> , not the comment objects themselves. During the window after an entry has been copied but before the table swap and backlog replay, the old table is still published for packet-side updates while the replacement-table entry already holds the same <code>ip_set_comment_rcu</code> pointer. If <code>xt_SET --add-set ... --exist</code> hits that old entry in this window, <code>mtype_add()</code> calls <code>ip_set_init_comment()</code> even though packet-side adds carry no comment payload. That call frees the shared comment through the old entry, so the replacement-table entry now holds a stale pointer. When the queued add is replayed on the new table, <code>mtype_add()</code> calls <code>ip_set_init_comment()</code> again and <code>strlen()</code> dereferences the stale pointer. Fix this in <code>mtype_add()</code> by skipping	2026-08-15	8.4	CVE-2026-74492

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ip_set_init_comment() when ext->target marks a packet-side add. Userspace adds still update comments, while packet-side adds can no longer free comment storage shared with a resize copy.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Clamp frame size in implicit-feedback mode snd_usb_handle_sync_urb() scales received sync packet sizes by the sender's stride and stores the result directly in out_packet->packet_size[i]. If a connected USB device sends an oversized sync packet, this frame count can exceed ep->maxframesize. The un-clamped frame count then propagates to the playback endpoint queue, potentially driving packet transfers beyond the endpoint's hardware frame limits. Cap the calculated frame count against ep->maxframesize in snd_usb_handle_sync_urb() to prevent oversized packets from entering the playback queue.	2026-08-15	8.4	CVE-2026-74497
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: HIDP: reject frames without a transaction header hidp_rcv_ctrl_frame() and hidp_rcv_intr_frame() read skb->data[0] before checking that the L2CAP SDU contains a transaction header. A connected HIDP peer can send an empty basic-mode SDU and make both paths use an uninitialized byte from skb tailroom. KMSAN reports the use in hidp_session_run(), with the uninitialized value originating in __alloc_skb() through vhci_write(). The control path produces two reports and the interrupt path produces one. The byte can also be controlled by a malformed lower-layer packet. If an HCI ACL packet contains an L2CAP PDU with a declared zero-length payload followed by an extra 0x15 byte, l2cap_rcv_acldata() reduces skb->len to the declared PDU length before dispatch. The current HIDP path nevertheless consumes the extra byte as HIDP_TRANS_HID_CONTROL HIDP_CTRL_VIRTUAL_CABLE_UNPLUG and terminates the HIDP session. With this change, the same packet is discarded and a subsequent feature report request succeeds. Pull the transaction header with skb_pull_data() and discard frames that do not contain it.	2026-08-15	8.8	CVE-2026-74508
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: Fix advertising data UAFs hci_find_adv_instance() returns an adv_info pointer that is valid only while hdev->lock is held. The advertising command-sync paths perform instance lookups without that lock and, in some cases, retain the pointer while waiting for a controller response. An advertising termination event can therefore interleave as follows: hci_cmd_sync_work hci_rx_work hci_find_adv_instance() __hci_cmd_sync_status() wait for controller reply hci_dev_lock() hci_remove_adv_instance() kfree(adv) adv->scan_rsp_changed = false KASAN reported: BUG: KASAN: slab-use-after-free in hci_set_ext_scan_rsp_data_sync+0x2e1/0x300 Write of size 1 at addr ffff88810a45d21d by task kworker/u17:0/88 Workqueue: hci0 hci_cmd_sync_work Call Trace: hci_set_ext_scan_rsp_data_sync+0x2e1/0x300 hci_schedule_adv_instance_sync+0x390/0x4c0 hci_cmd_sync_work+0x173/0x300 Allocated by task 87: hci_add_adv_instance+0x538/0xac0 add_advertising+0x885/0x1160 Freed by task 89: kfree+0x131/0x3c0 hci_remove_adv_instance+0x1d8/0x3b0 hci_le_ext_adv_term_evt+0x17b/0x730 Protect the instance lookup and payload construction in the extended advertising, scan response, and periodic advertising data paths. Snapshot the advertising parameters under hdev->lock, but release the lock before waiting for the controller. Clear advertising-data dirty bits before issuing their commands and restore them after a failure using a fresh lookup. Likewise, update the reported transmit power through a fresh lookup after the parameter command completes. No adv_info pointer then survives an HCI command wait.	2026-08-15	8.8	CVE-2026-74509
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: pci: Reject adapter interrupt forwarding if already enabled The MPCIFC instruction doesn't allow registering adapter interrupts without first unregistering. So reject any request to enable interrupt forwarding if its already enabled for the zPCI device. This also fixes overwriting and thus leaking resources when the ioctl is called multiple times for the same device.	2026-08-15	8.8	CVE-2026-74515
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: SVM: Update x2APIC MSR intercepts if AVIC is inhibited while L2 is active Always update x2APIC MSR intercepts for L1 when AVIC is deactivated, even if L2 is active and KVM is using a separate MSR bitmap to run L2. If AVIC is fully enabled prior to running L2, and is then inhibited while L2 is active (for a VM-scoped inhibit), then KVM will run L1 with AVIC disabled, but with x2APIC MSR intercepts disabled, i.e. will allow L1 to read most of the host's APIC state, send arbitrary interrupts, change task priority, and ultimately trivially DoS the host. E.g. sending a self-IPI in L1 on	2026-08-15	8.2	CVE-2026-74516

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HYPERV_REENLIGHTENMENT_VECTOR, 0xee, with CONFIG_HYPERV=n in the host kernel as a "safe" PoC, yields: Spurious interrupt (vector 0xee) on CPU#425. Aced And hacking KVM to abuse kvm_set_posted_intr_wakeup_handler() to register a handler and WARN on POSTED_INTR_WAKEUP_VECTOR yields: -----[cut here]----- WARNING: arch/x86/kvm/svm/svm.c:5594 at pi_wakeup_handler+0x9/0x10 [kvm_amd], CPU#156: nested_x2apic_t/316940 CPU: 156 UID: 0 PID: 316940 Comm: nested_x2apic_t Tainted: G S U Tainted: [S]=CPU_OUT_OF_SPEC, [U]=USER Hardware name: Google Astoria-Turin/astoria, BIOS 0.20260209.0-0 02/09/2026 RIP: 0010:pi_wakeup_handler+0x9/0x10 [kvm_amd] Call Trace: <IRQ> sysvec_kvm_posted_intr_wakeup_ipi+0x64/0x80 </IRQ> <TASK> asm_sysvec_kvm_posted_intr_wakeup_ipi+0x1a/0x20 RIP: 0010:vcpu_run+0x1430/0x1e40 [kvm] kvm_arch_vcpu_ioctl_run+0x2c1/0x600 [kvm] kvm_vcpu_ioctl+0x580/0x6b0 [kvm] __se_sys_ioctl+0x6d/0xb0 do_syscall_64+0x10a/0x480 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x46ff4b </TASK> ---[end trace 0000000000000000]---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/iommu: Fix IOPF group ownership UAF iopf_group_alloc() links each last-page IOPF group into the generic IOPF pending list before invoking the domain fault handler. iommu_fault_iopf_handler() also queued an accepted group in the IOMMUFD deliver list without removing it from the generic pending list. When detach or HWPT replacement drops the device's IOPF reference count to zero, an IOMMU driver may call iopf_queue_remove_device(). That function responds to and frees groups through the generic pending list without removing the same groups from IOMMUFD's deliver list or response xarray. A later read, response, or cleanup can then access the freed group and cause a UAF. Fix this by dequeuing an accepted group from the generic pending list before IOMMUFD queues it for userspace response. Make iopf_group_response() send a response regardless of pending-list membership, so the dequeued group can still be completed by IOMMUFD.	2026-08-15	8.8	CVE-2026-74520
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in __close_file_table_ids() A ksmbd_file can remain alive after logical close while another session holds a temporary reference obtained through ksmbd_lookup_fd_inode(). ksmbd_close_fd() currently marks the file closed and drops the idr-owned reference, but leaves the pointer published in the closing session's idr until the final reference is dropped. If the foreign holder performs the final ksmbd_fd_put(), __put_fd_final() supplies the foreign session's file table to __ksmbd_close_fd(). The object is then freed without being removed from its owner's idr, and the owner session later dereferences the stale pointer during file-table teardown. Remove the volatile id from the owner's idr while ksmbd_close_fd() still holds that table's lock, and clear volatile_id before dropping the idr-owned reference. A later foreign final put then only performs physical destruction and cannot remove the object from the wrong table.	2026-08-15	8.8	CVE-2026-74522
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: octeonx2-af: Block VFs from clobbering special CGX PKIND state PF and VF NIX LFs that share a CGX LMAC reuse the same hardware PKIND programming. When HiGig2 or EDSA parsing is enabled, a VF NIX LF alloc must not reset the LMAC RX PKIND or default TX parse config over the PF setup. Add cgx_get_pkind() and rvu_cgx_is_pkind_config_permitted() so VFs skip cgx_set_pkind(), rvu_npc_set_pkind(), and NIX_AF_LFX_TX_PARSE_CFG updates when the LMAC is using NPC_RX_HIGIG_PKIND or NPC_RX_EDSA_PKIND.	2026-08-15	8.8	CVE-2026-74527
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: hold conn in hci_past_sync() callback Avoids giving freed pointers to hci_conn_valid(), which kcalloc may have reused. Hold refcount to avoid that.	2026-08-15	8	CVE-2026-74528
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: hold conn in hci_connect_big_sync() callback There is theoretical UAF if the conn is freed while the hci_sync task is running. Hold refcount to avoid that. Handle NULL hcon, return 0 + do nothing to match the previous behavior.	2026-08-15	8.8	CVE-2026-74530
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_conn: hold conn reference in abort_conn_sync() There is theoretical UAF if the conn is freed while the hci_sync task is running. Hold refcount to avoid that.	2026-08-15	8.8	CVE-2026-74531
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: fix race of kfree vs kref_get_unless_zero hci_conn::iso_data is accessed and modified without lock or RCU. This leads to a race [Task hdev->workqueue] [Task 2] iso_rcv iso_conn_put(conn) conn = LOAD hcon->iso_data iso_conn_free(conn)	2026-08-15	8.8	CVE-2026-74533

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	iso_conn_hold_unless_zero(conn) hcon->iso_data = NULL kfree(conn) kref_get_unless_zero(&conn->ref) /* UAF */ and also to races in iso_conn_add() vs. iso_conn_free(). Fix by adding spinlock hci_conn::proto_lock and using it to guard hci_conn::iso_data.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: fix refcounting of iso_conn iso_conn_del() and iso_chan_del() have a race that results to double-put of iso_conn: [Task hdev->workqueue] [Task 2] iso_conn_del iso_chan_del iso_conn_hold_unless_zero iso_conn_lock iso_conn_lock conn->sk = NULL iso_conn_unlock sk = iso_sock_hold(conn) <-----' if (!sk) iso_conn_put iso_conn_put iso_conn_put /* UAF */ The extra put for !sk in iso_conn_del() is currently required since failing iso_chan_add() may leave iso_conn not associated with any sk. Fix by having iso_pi(sk)->conn own refcount when non-NULL, so iso_conn_del does not need to put it. Adjust the iso_conn_add() refcounting so that conn is put if it does not get associated with an sk.	2026-08-15	8.8	CVE-2026-74534
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: avoid deadlocks in iso_sock_timeout iso_sock_timeout() takes lock_sock, so sync disabling the timer while holding that lock may deadlock. iso_sock_timeout() may also run concurrently with iso_conn_del(), which leads to UAF [Task 1] [Task hdev->workqueue] iso_sock_timeout iso_conn_del iso_conn_hold_unless_zero iso_chan_del `-----> iso_conn_put caller frees hcon iso_conn_put iso_conn_free conn->hcon->iso_data = NULL; /* UAF */ Fix the deadlock by removing the disable from the lock_sock sections. Move the timer from iso_conn to iso_pinfo to decouple it from iso_conn which may need to be freed in lock_sock section. Convert some of the clear_timer to disable_timer.	2026-08-15	8.8	CVE-2026-74535
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: hold sk properly in iso_conn_ready sk deref in iso_conn_ready must be done either under conn->lock, or holding a refcount, to avoid concurrent close. conn->sk is currently accessed without either: [Task 1] [Task 2] iso_sock_release iso_conn_ready sk = conn->sk lock_sock(sk) conn->sk = NULL lock_sock(sk) release_sock(sk) iso_sock_kill(sk) UAF on sk deref Fix possible UAF by holding sk refcount in iso_conn_ready(). Also recheck after lock_sock that the socket is still valid. Adjust locking so conn->sk is cleared only under lock_sock.	2026-08-15	8.8	CVE-2026-74537
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: lock sk in iso_connect_ind Accessing iso_pi(sk)->conn requires lock_sock, which is not taken in the "ev3" part of iso_connect_ind. It may also be NULL if socket has transitioned away from the LISTEN/CONNECT states before locking. Fix by adding lock/release. Recheck hcon is valid after lock acquire where needed.	2026-08-15	8.8	CVE-2026-74538
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: lock sk in iso_sock_getname Accessing iso_pi(sk)->conn requires lock_sock, which is not held here. Fix by adding the lock/release.	2026-08-15	8	CVE-2026-74539
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: fix UAF in l2cap_le_connect_rsp l2cap_le_connect_rsp() obtains a channel via __l2cap_get_chan_by_ident() but neither holds a reference nor uses l2cap_chan_hold_unless_zero() before locking and operating on it. A concurrent l2cap_chan_del() triggered by a remote disconnect can free the channel between the lookup and l2cap_chan_lock(), causing a use-after-free. The BR/EDR counterpart l2cap_connect_rsp() and the sibling handler l2cap_le_command_rej() already use l2cap_chan_hold_unless_zero() to safely hold a reference, but l2cap_le_connect_rsp() was left unprotected. Fix by adding l2cap_chan_hold_unless_zero() after the ident lookup and l2cap_chan_put() on the exit path, consistent with other L2CAP response handlers.	2026-08-15	8.8	CVE-2026-74540
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: clear iso_data always when detaching conn from hcon When setting conn->hcon = NULL, also conn->hcon->iso_data = NULL is necessary, otherwise later iso_conn_free() will UAF. Fix clearing of iso_data in iso_sock_disconn() Fixes KASAN: slab-use-after-free in iso_conn_hold_unless_zero on iso_sock_release() followed by hci_abort_conn_sync().	2026-08-15	8.8	CVE-2026-74541
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix out-of-bounds clear_bit in ath12k_mac_dp_peer_cleanup() ath12k_mac_dp_peer_cleanup() clears the ML peer ID slot on the free_ml_peer_id_map bitmap by indexing it with dp_peer->peer_id. That is wrong: dp_peer->peer_id for an MLO peer always carries the ATH12K_PEER_ML_ID_VALID bit (BIT(13)), so clear_bit() is invoked with index >= 0x2000, which is far outside the bitmap of ATH12K_MAX_MLO_PEERS (256) bits and corrupts memory adjacent to	2026-08-15	8.8	CVE-2026-74554

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ah->free_ml_peer_id_map. The intended bitmap entry also never gets cleared, so subsequent ath12k_peer_ml_alloc() calls eventually run out of IDs. The ID without the VALID bit is what ath12k_peer_ml_alloc() returned and is stored in ahsta->ml_peer_id. Use that instead. While there, also reset ahsta->ml_peer_id to ATH12K_MLO_PEER_ID_INVALID so the bitmap and ahsta->ml_peer_id stay in sync. Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.1.c5-00302-QCAHMTSWPL_V1.0_V2.0_SILICONZ-1.115823.3			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nexthop: avoid unlocked f6i_list walk in nh_rt_cache_flush nh_rt_cache_flush() walks nh->f6i_list during an RTNL-serialized nexthop replace without holding nh->lock, racing the unlocked IPv6 route add/delete that mutate the list under nh->lock and free fib6_info entries (nh_rt_cache_flush() is inlined into rtm_new_nexthop()): BUG: KASAN: slab-use-after-free in nh_rt_cache_flush (net/ipv4/nexthop.c:2243) Read of size 8 at addr ffff888012953e18 by task exploit/146 nh_rt_cache_flush (net/ipv4/nexthop.c:2243) replace_nexthop (net/ipv4/nexthop.c:2610) rtm_new_nexthop (net/ipv4/nexthop.c:3323) rtnetlink_rcv_msg (net/core/rtnetlink.c:7076) Unlike the other f6i_list walks, this one bumps each route's sernum via fib6_update_sernum_upto_root(), which needs tb6_lock; taking nh->lock around it would invert the established tb6_lock -> nh->lock order and deadlock. As the only purpose is to invalidate cached dsts, bump the IPv6 sernum for the whole netns with rt_genid_bump_ipv6() instead, mirroring the rt_cache_flush() already done for IPv4 just above.	2026-08-15	8.8	CVE-2026-74561
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nexthop: take nh->lock for f6i_list walks in replace check and notify fib6_check_nh_list() and __nexthop_replace_notify() walk nh->f6i_list during an RTNL-serialized nexthop replace without holding nh->lock. IPv6 RTM_NEWROUTE/RTM_DELROUTE run without RTNL and mutate that list under nh->lock (fib6_add_rt2node_nh(), fib6_purge_rt()), so both walks race a concurrent route delete that unlinks and frees a fib6_info: BUG: KASAN: slab-use-after-free in rt6_fill_node.isra.0 (net/ipv6/route.c:5799) Read of size 4 at addr ffff888014607e64 by task exploit/143 rt6_fill_node.isra.0 (net/ipv6/route.c:5799) fib6_rt_update (net/ipv6/route.c:6412) __nexthop_replace_notify (net/ipv4/nexthop.c:2542) rtm_new_nexthop (net/ipv4/nexthop.c:2554) rtnetlink_rcv_msg (net/core/rtnetlink.c:7076) BUG: KASAN: slab-use-after-free in fib6_check_nh_list (net/ipv4/nexthop.c:1605) Read of size 8 at addr ffff888014a7d068 by task exploit/142 fib6_check_nh_list (net/ipv4/nexthop.c:1605) rtm_new_nexthop (net/ipv4/nexthop.c:2575) rtnetlink_rcv_msg (net/core/rtnetlink.c:7076) Both walks only read the entries and take no tb6_lock, so protect them with nh->lock; fib6_rt_update() uses gfp_any(), which returns GFP_ATOMIC under the lock.	2026-08-15	8.8	CVE-2026-74562
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Prevent XDomain delayed work use-after-free on disconnect tb_xdp_handle_request() runs on system_wq and queues xd->state_work via queue_delayed_work() in three request handlers: PROPERTIES_CHANGED_REQUEST, UUID_REQUEST (via start_handshake), and LINK_STATE_CHANGE_REQUEST. Similarly, update_xdomain() queues xd->properties_changed_work when local properties change. Concurrently, tb_xdomain_remove() calls stop_handshake() which does cancel_delayed_work_sync() on both delayed works. Later, tb_xdomain_unregister() calls device_unregister() which eventually frees the xdomain. Since commit 559c1e1e0134 ("thunderbolt: Run tb_xdp_handle_request() in system workqueue") moved the request handler off tb->wq, the handler and the remove path are no longer serialized. If queue_delayed_work() executes after cancel_delayed_work_sync() but before the xdomain is freed, the delayed work fires on a freed object. Add xd->removing that tb_xdomain_remove() sets under xd->lock before calling stop_handshake(). Each external queue site holds the same lock and checks removing before calling queue_delayed_work(). This provides the mutual exclusion needed: either the queue site acquires the lock first and queues work that the subsequent cancel will see, or the remove path acquires the lock first and the queue site observes removing == true and skips the queue.	2026-08-15	8.8	CVE-2026-74575
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: audit: fix recursive locking deadlock in audit_dupe_exe() A deadlock occurs in the audit subsystem when duplicating executable-related rules. When a file is moved (e.g., via do_renameat2()), the VFS layer locks the parent directory (I_MUTEX_PARENT), which synchronously triggers an fsnotify_move event. If an existing executable	2026-08-10	7.5	CVE-2026-68096

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	audit rule matches the file being moved, the audit subsystem catches this event and calls audit_dupe_exe() to duplicate the watch and update the rule. Then, audit_alloc_mark() would call kern_path_parent() to resolve the path, leading to a blind attempt to acquire the exact same I_MUTEX_PARENT lock already held by the task, resulting in the following recursive locking deadlock: <pre>===== WARNING: possible recursive locking detected 6.12.0-55.27.1.el10_0.x86_64+debug #1 Not tainted ----- ----- mv/5099 is trying to acquire lock: ffff888132845358 (&inode->i_sb->s_type->i_mutex_dir_key/1){+..}-{3:3}, at: __kern_path_locked+0x10a/0x2f0 but task is already holding lock: ffff888132846b58 (&inode->i_sb->s_type->i_mutex_dir_key/1){+..}-{3:3}, at: lock_two_directories+0x13f/0x2b0 other info that might help us debug this: Possible unsafe locking scenario: CPU0 ---- lock(&inode->i_sb->s_type->i_mutex_dir_key/1); lock(&inode->i_sb->s_type->i_mutex_dir_key/1); *** DEADLOCK *** May be due to missing lock nesting notation 6 locks held by mv/5099: #0: ffff888112a9c440 (sb_writers#13) at: do_renameat2+0x34c/0xabc0 #1: ffff888112a9c790 (&type->s_vfs_rename_key#3) at: do_renameat2+0x415/0xabc0 #2: ffff888132846b58 (&inode->i_sb->s_type->i_mutex_dir_key/1) at: lock_two_directories+0x13f/0x2b0 #3: ffff888132845358 (&inode->i_sb->s_type->i_mutex_dir_key/5) at: lock_two_directories+0x175/0x2b0 #4: ffffffff3a1fb10 (&fsnotify_mark_srcu) at: fsnotify+0x454/0x28a0 #5: ffffffffaf886230 (audit_filter_mutex) at: audit_update_watch+0x36/0x11e0 stack backtrace: Call Trace: <TASK> dump_stack_lvl+0x6f/0xb0 print_deadlock_bug.cold+0xbd/0xca validate_chain+0x83a/0xf00 __lock_acquire+0xcac/0x1d20 lock_acquire.part.0+0x11b/0x360 down_write_nested+0x9f/0x230 __kern_path_locked+0x10a/0x2f0 kern_path_locked+0x26/0x40 audit_alloc_mark+0xfb/0x4f0 audit_dupe_exe+0x6c/0xe0 audit_dupe_rule+0x6c2/0xc00 audit_update_watch+0x4cc/0x11e0 audit_watch_handle_event+0x12c/0x1b0 send_to_group+0x5d0/0x8b0 fsnotify+0x615/0x28a0 fsnotify_move+0x1d8/0x630 vfs_rename+0xdcd/0x1df0 do_renameat2+0x9d4/0xabc0 __x64_sys_renameat+0x192/0x260 do_syscall_64+0x92/0x180 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7f0491fe8c4e Code: 0f 1f 40 00 48 8b 15 c1 e1 16 00 f7 d8 64 89 02 b8 ff ff ff c3 66 0f 1f 44 00 00 f3 0f 1e fa 49 89 ca b8 08 01 00 00 0f 05 <48> 3d 00 f0 ff ff 77 0a c3 66 0f 1f 84 00 00 00 00 00 48 8b 15 89 RSP: 002b:00007ffc7210bf38 EFLAGS: 00000246 ORIG_RAX: 0000000000000108 RAX: ffffffffda RBX: 0000000000000000 RCX: 00007f0491fe8c4e RDX: 0000000000000003 RSI: 00007ffc7210e6c8 RDI: 00000000fffff9c RBP: 0000000000000000 R08: 0000000000000000 R09: 0000000000000001 R10: 00005575eb2dae2a R11: 0000000000000246 R12: 00005575eb2dae2a R13: 00007ffc7210e6c8 R14: 0000000000000003 R15: 00000000fffff9c </TASK> The aforementioned deadlock can be consistently reproduced by running the script below: audit-dupe-exe-deadlock.sh ----- #!/bin/bash auditctl -D mkdir -p /tmp/foo touch /tmp/file auditctl -a always,exit -F exe=/tmp/file -F path=/tmp/file -S all -k dr mv /tmp/file /tmp/foo/file rm -rf /tmp/foo This patch fixes the issue by introducing struct audit_watch_ctx to pass the fsnotify event context down to audit_alloc_mark(). By utilizing the already-resolved directory inode provided by the event, we bypass the kern_path_parent() path resol ---truncated---</pre>			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: reject mapping a reserved doorbell to a new queue When creating an user-queue, the user space provides a doorbell BO handle and an offset within the bo to obtain a doorbell. However current implementation using xa_store_irq() to store a doorbell, which allows a later queue created with the same BO and offset parameters to overwrite an existing queue and doorbell mapping. This can cause problems like misrouting fence IRQ processing to a wrong queue, and mislead the cleanup process of one queue erasing the mapping of another queue. This commit fixes this issue by replacing xa_store_irq with xa_insert_irq, which rejects mapping a reserved doorbell to a newly created queue (cherry picked from commit 6244eae22966350db52faf9c1369d3b2ffc5de4e)	2026-08-10	7.1	CVE-2026-68103
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: invoke pm_genpd_remove() before freeing genpd Call pm_genpd_remove() to unregister from global list prior to releasing acp_genpd memory, and clear the pointer after free. (cherry picked from commit cd8650d7a91ee8b768e202354672553faa5cc1f2)	2026-08-10	7.8	CVE-2026-68104

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix division by zero with invalid uvd dimensions When width or height is less than 16, width_in_mb or height_in_mb becomes 0, leading to fs_in_mb being 0. This causes a division by zero when calculating num_dpb_buffer in H264 and H264 Perf decode paths. Add validation to reject frames with width < 16 or height < 16 before performing any calculations that depend on these values. V2: Format change - move up all variable definitions. V3: Use warn_once to avoid spam. (cherry picked from commit 3e41d26c70b0a459d041cc19482a226c4b7423cb)	2026-08-10	7.8	CVE-2026-68106
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: mdb: Fix source list corruption on a failed replace When replacing the source list of an MDB remote entry, all existing sources are first marked for deletion and vxlan_mdb_remote_srcs_add() is then called to add the new source list. Sources present in the new list have their deletion mark cleared, and any sources left marked afterwards are removed. If vxlan_mdb_remote_srcs_add() fails partway through, its error path deletes all entries on the remote's source list. That rollback is only correct for its other caller, vxlan_mdb_remote_add(), where the remote was just allocated and the list contains solely entries added during the call. On the replace path the list also holds pre-existing sources, so a failed replace tears them down together with their (S, G) forwarding entries instead of leaving the entry unchanged. This is reachable from an existing (*, G) remote. An EXCLUDE filter that loses sources starts forwarding traffic that should be blocked, while an INCLUDE filter that loses sources drops traffic that should be forwarded. Mark entries created during the current pass with a new VXLAN_SGRP_F_NEW flag. On failure, delete only those entries and clear the deletion mark on the pre-existing ones, so a failed replace leaves the source list untouched. Retain the flag until the whole operation succeeds and then clear it. Also stop vxlan_mdb_remote_src_add() from deleting a pre-existing entry it only looked up when adding that entry's forwarding entry fails.	2026-08-10	7.9	CVE-2026-68116
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: initialize standalone TCP-AO response padding tcp_v4_send_ack() and tcp_v6_send_response() construct standalone TCP responses with TCP-AO options. The option length carries the actual MAC length, but the TCP header length includes the option rounded up to a four-byte boundary. tcp_ao_hash_hdr() writes the MAC only. Thus, when the MAC length is not four-byte aligned, the one to three bytes after the MAC are left uninitialized and may be transmitted. For the normal TCP-AO hashing mode, those bytes also have to be initialized before computing the MAC. Initialize only the alignment padding in the TCP-AO branches, before hashing the header. Use TCPOPT_NOP, as in the normal TCP-AO output path. This avoids adding work to non-AO TCP responses while preserving a valid authenticated header.	2026-08-10	7.5	CVE-2026-68119
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rtase: Workaround for TX hang caused by hardware packet parsing The hardware performs packet parsing before packet transmission. Parsing incomplete IPv4, IPv6, TCP, or UDP headers may trigger a TX hang because the hardware parser expects additional protocol header data that is not present in the packet. The hardware performs additional PTP parsing on UDP packets identified by destination ports 319/320 at the expected UDP destination port offset. If such a packet has transport data smaller than RTASE_MIN_PAD_LEN, the hardware parser expects additional packet data and may trigger a TX hang. To avoid these hardware issues, the driver applies the following workarounds. Drop malformed packets that may trigger this hardware issue before transmission. For IPv4 non-initial fragments, the hardware does not check the fragment offset before parsing the expected transport header location. As a result, these packets are still subject to transport header parsing even though they do not contain a transport header. If the transport data is shorter than the minimum transport header required by the hardware parser, pad the transport data to the minimum transport header length required by the hardware parser. Packets that also match the hardware PTP parsing conditions continue to follow the corresponding workaround. For IPv6 fragmented packets, neither of the above hardware issues occurs because the hardware only continues packet parsing when the IPv6 Base Header Next Header field directly indicates UDP. Packets carrying a Fragment Header do not continue through the subsequent packet parsing stages. For packets identified for hardware PTP parsing, pad the transport data so it reaches RTASE_MIN_PAD_LEN before transmission.	2026-08-10	7.5	CVE-2026-68120
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: pppoe: reload header pointer after dev_hard_header() pppoe_sendmsg() saves a pointer to the	2026-08-10	7.8	CVE-2026-68121

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	PPPoE header before calling dev_hard_header(). Device header callbacks are allowed to reallocate the skb head, invalidating pointers into it. This can happen when a send is blocked in copy_from_user() while the first non-Ethernet port is added to an empty team device. The team's delegated GRE header callback then expands the skb head. PPPoE subsequently writes six bytes through the stale pointer into the freed head. Reload the PPPoE header through the skb's network-header offset after device header creation. pskb_expand_head() updates that offset when it relocates the head.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gve: fix Rx queue stall on alloc failure When the system is under extreme memory pressure, page allocations can fail during the Rx buffer refill loop. If the number of buffers posted to hardware falls below a critical low threshold and the refill loop exits due to allocation failures, the queue can stall: 1. The device drops incoming packets because there are no descriptors. 2. Since no packets are processed, no Rx completions are generated. 3. Because no completions occur, NAPI is never scheduled, preventing the refill loop from running again even after memory is freed. This results in a permanent queue stall. Resolve this by introducing a starvation recovery timer for each Rx queue. If the number of buffers posted to hardware falls below a critical low threshold, start a timer to periodically reschedule NAPI. Once NAPI runs and successfully refills the queue above the threshold, the timer is not rescheduled. The threshold is set to 32 because a single maximum-sized Receive Segment Coalescing (RSC) packet can consume up to 19 descriptors in the Rx path. Lower thresholds (such as 8 or 16) would be insufficient to process a complete maximum-sized RSC packet, risking packet drops or unexpected hardware behavior under memory pressure. Setting the threshold to 32 guarantees a safe margin to handle at least one full RSC packet.	2026-08-10	7.5	CVE-2026-68129
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rbd: Reset positive result codes to zero in object map update path In a reply message to an RBD request, a positive result code indicates a data payload, which is not allowed for writes. While rbd_osd_req_callback() already resets a positive result code for writes to zero, rbd_object_map_callback() does not. This allows a corrupted reply to an object map update to trigger the rbd_assert(*result < 0) in __rbd_obj_handle_request(). This happens, because rbd_object_map_callback() calls rbd_obj_handle_request() -> __rbd_obj_handle_request() and passes this positive result code. From __rbd_obj_handle_request(), rbd_obj_advance_write() is called, which leaves the positive result code unchanged and returns true. Therefore, the if(done && *result) branch is executed in __rbd_obj_handle_request() and the assertion triggers. This patch fixes the issue by adjusting the logic in the rbd_object_map_callback() path. A positive result code for an object map update is now reset to zero (similar to rbd_osd_req_callback()), and the message is subsequently handled the same way as if the result code was zero from the beginning. Additionally, a WARN_ON_ONCE() is added for this case.	2026-08-10	7.5	CVE-2026-68131
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ptp: ptp_s390: Add missing facility check Only register the physical clock when facility 28 is installed and PTFF QAF returns that PTFF QPT is available.	2026-08-10	7.3	CVE-2026-68134
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: serialize qdisc_rtab_list against concurrent get/put qdisc_get_rtab() and qdisc_put_rtab() mutate the process-global singly linked list qdisc_rtab_list and a plain non-atomic 'int refcnt' with no lock. This was only safe because every caller historically held the RTNL mutex, which serialized all rate-table lookups, inserts and frees. That invariant no longer holds. cls_flower sets TCF_PROTO_OPS_DOIT_UNLOCKED, so tc_new_tfilter() keeps rtnl_held == false for it and sets TCA_ACT_FLAGS_NO_RTNL. That flag propagates through tcf_exts_validate_ex() -> tcf_action_init() -> tcf_action_init_1() -> tcf_police_init(), which calls qdisc_get_rtab()/qdisc_put_rtab() with the RTNL mutex NOT held. Two RTM_NEWTFILTER requests on different CPUs, each adding a flower filter with a police action carrying the same rate, then race on qdisc_rtab_list and on the non-atomic refcnt, leading to a use-after-free / double-free of the kcalloc-2k struct qdisc_rate_table. qdisc_rtab_list is a single global (not per-netns), so the corrupted object is shared system-wide. BUG: KASAN: slab-use-after-free in qdisc_put_rtab+0x12f/0x160 qdisc_put_rtab+0x12f/0x160 tcf_police_init+0xda9/0x1590 tcf_action_init_1+0x460/0x6b0 tcf_action_init+0x439/0xa40 tcf_exts_validate_ex+0x42d/0x550 fl_change+0xddd/0x7da0 tc_new_tfilter+0xaa7/0x2420 rtnetlink_rcv_msg+0x95e/0xe90 which belongs to the cache kcalloc-2k of size	2026-08-10	7.8	CVE-2026-68138

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2048 Protect qdisc_rtab_list and the refcount with a dedicated spinlock. The (sleeping, GFP_KERNEL) allocation in qdisc_get_rtab() is performed before taking the lock; if a concurrent inserter added an identical table in the meantime the freshly allocated one is freed under the lock, so no duplicate is leaked. qdisc_put_rtab() now decrements the refcount and unlinks under the same lock.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/af_iucv: fix NULL deref in afiucv_hs_callback_syn() afiucv_hs_callback_syn() allocates the child socket with GFP_ATOMIC. If the allocation fails, nsk is NULL. The connection-refused path is entered when the listen state check fails, the accept backlog is full, or nsk is NULL. The code unconditionally calls iucv_sock_kill(nsk) in that path. iucv_sock_kill() does not accept a NULL socket pointer and immediately dereferences sk via sock_flag(sk, SOCK_ZAPPED). When nsk is NULL, calling iucv_sock_kill(nsk) results in a NULL pointer dereference. Only call iucv_sock_kill() when a child socket was successfully allocated.	2026-08-10	7.5	CVE-2026-68141
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: slip: serialize receive against buffer reallocation sl_realloc_bufs() replaces rbuff and updates buffsize while holding sl->lock. slip_receive_buf() reads those fields and writes through rbuff without holding the lock. An MTU change can therefore race with receive processing. An MTU shrink can expose the new smaller rbuff with the old larger bound, causing an out-of-bounds write. A receive callback which already loaded the old rbuff can instead continue writing after that buffer has been freed. Serialize receive processing with sl_realloc_bufs() by holding sl->lock while consuming each receive batch.	2026-08-10	7.8	CVE-2026-68143
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iomap: fix out-of-bounds bitmap_set() with zero-length range ifs_set_range_dirty() and ifs_set_range_uptodate() compute last_blk as (off + len - 1) >> i_blkbits. When off is 0 and len is 0, the unsigned subtraction underflows to SIZE_MAX, producing a huge last_blk and nr_blks value that causes bitmap_set() to write far beyond the ifs->state allocation. Regarding ifs_set_range_uptodate(), it is temporarily safe because len cannot be passed in as 0. However, for ifs_set_range_dirty() this is reachable from __iomap_write_end(): when copy_folio_from_iter_atomic() returns 0 (e.g. user buffer fault) and the folio is already uptodate, the guard at the top of __iomap_write_end() does not trigger because !folio_test_uptodate() is false, and iomap_set_range_dirty() is called with copied == 0. Add a !len guard to both functions before the computation, so that a zero-length range is a no-op.	2026-08-10	7.8	CVE-2026-68145
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fscrypt: Avoid dynamic allocation in fscrypt_get_devices() When a blk_crypto_key starts being used or is evicted, fs/crypto/ calls fscrypt_get_devices() to get the filesystem's list of block devices, then iterates over them and calls blk_crypto_config_supported(), blk_crypto_start_using_key(), or blk_crypto_evict_key() on each one. Currently, the block device pointers are placed in a dynamically allocated array. This dynamic allocation is problematic because: - It can fail, especially at the fscrypt_destroy_inline_crypt_key() call site when it's invoked for inode eviction under direct reclaim. - fscrypt_destroy_inline_crypt_key() doesn't handle the failure. It just zeroizes and frees the blk_crypto_key without calling blk_crypto_evict_key(). That causes a use-after-free. For now, let's fix this in the straightforward and easily-backportable way by switching to an on-stack array. Currently the fscrypt multi-device functionality is used only by f2fs, which has a hardcoded limit of 8 block devices. An on-stack array works fine for that. (Of course, this solution won't scale up to large number of block devices. For that we'd need a different solution, like moving the block device iteration into the filesystem. Or in the case of btrfs, which will only support blk-crypto-fallback, we should make it just call blk-crypto-fallback directly, so the block devices won't be needed.)	2026-08-10	7.8	CVE-2026-68147
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fscrypt: Add missing superblock check in find_or_insert_direct_key() The legacy 'fscrypt_direct_keys' table caches master keys that are used by v1 encryption policies that have FSCRYPT_POLICY_FLAG_DIRECT_KEY. It's just a global table for all filesystems (since the keys can be provided by the legacy process-subscribed keyrings mechanism, which makes it difficult to reuse super_block::s_master_keys). The entries in it ('struct fscrypt_direct_key') do contain a super_block pointer, though, for passing to fscrypt_destroy_inline_crypt_key() when the last inode that references the key is evicted. However, when finding the fscrypt_direct_key for an inode, we weren't actually comparing the super_block pointer. As a result, inodes with different super_blocks could point to the same fscrypt_direct_key. That could extend the	2026-08-10	7.8	CVE-2026-68148

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lifetime of a fscrypt_direct_key beyond the super_block it points to, causing a use-after-free later. Fix this by creating distinct fscrypt_direct_key structs for distinct super_block structs. Note that this problem doesn't exist in the v2 policy equivalent ("per-mode keys"), since the data structures there are per super_block.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: amt: fix use-after-free in AMT delayed works When an AMT device is removed, pending delayed works can still access the freed amt_dev structure, which may result in kernel crashes or memory corruption. amt_dev_stop() cancels req_wq and discovery_wq with cancel_delayed_work_sync(), but these works can be scheduled again from event_wq after the cancellation. This allows delayed works to access the freed amt_dev structure after the netdev has been released. The following is a simple race scenario: CPU0 CPU1 amt_dev_stop() cancel_delayed_work_sync() amt_event_work() mod_delayed_work(req_wq) free netdev req_wq accesses freed amt_dev Use disable_delayed_work_sync() in amt_dev_stop() to prevent req_wq and discovery_wq from being queued again and wait for running work items to complete. The delayed works are disabled after initialization in amt_newlink() and enabled only when the device is successfully opened. This keeps the delayed work lifecycle synchronized with the lifetime of the AMT device.	2026-08-10	7.8	CVE-2026-68152
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: remove debugfs files before client teardown ceph_destroy_client() tears down the monitor client before removing the per-client debugfs files. A concurrent read of the monmap debugfs file can enter monmap_show() after ceph_monc_stop() has freed monc->monmap, triggering a use-after-free. Remove the debugfs files before stopping the OSD and monitor clients. debugfs_remove() drains active handlers and prevents new accesses, so the debugfs callbacks can no longer race the rest of client teardown.	2026-08-10	7.8	CVE-2026-68153
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: Reject monmaps advertising zero monitors A message of type CEPH_MSG_MON_MAP contains a monmap that is sent from a monitor to the client. This monmap contains information about the existing monitors in the cluster. Currently, a monmap indicating that there are zero monitors in the cluster is treated as valid. However, it is impossible to have zero monitors in the cluster and still receive a valid monmap from a monitor. Therefore, such a monmap must be corrupted and should be treated as invalid. Furthermore, a monmap with a monitor count of zero can subsequently crash the client when attempting to open a session with a monitor in __open_session(). This happens because the "BUG_ON(monc->monmap->num_mon < 1)" assertion in pick_new_mon() is triggered. This patch extends a check in ceph_monmap_decode() to also reject arriving mon_maps with num_mon == 0 rather than only with num_mon > CEPH_MAX_MON. [idryomov: drop "log output for unusual values of num_mon" part]	2026-08-10	7.5	CVE-2026-68155
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: guard missing CRUSH type name lookup Localized read selection can walk a parent bucket whose name exists in the CRUSH map while its type has no matching entry in type_names. get_immediate_parent() then dereferences a NULL type_cn and passes an invalid pointer into strcmp(), causing a null-ptr-deref. Skip such malformed parent buckets unless both the bucket name and type name metadata are present. This keeps malformed hierarchy data from crashing locality lookup and safely falls back to "not local". [idryomov: add WARN_ON_ONCE]	2026-08-10	7.5	CVE-2026-68157
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: avoid auth_enable sysctl UAF during netns teardown proc_sctp_do_auth() updates the SCTP control socket after changing net.sctp.auth_enable. The handler gets the per-net SCTP state from ctl->data, so an already opened sysctl file can still target a network namespace while that namespace is being torn down. SCTP previously registered its per-net sysctls from sctp_defaults_init(), while the control socket is created later from sctp_ctrlsock_init(). This exposed a window during initialization where auth_enable was writable before net->sctp.ctl_sock existed, and a teardown window where auth_enable stayed writable after inet_ctl_sock_destroy() had released the control socket. Move the per-net SCTP sysctl registration into sctp_ctrlsock_init() after sctp_ctl_sock_init() succeeds, and unregister the sysctl table before destroying the control socket in sctp_ctrlsock_exit(). If sysctl registration fails after the control socket was created, destroy the control socket in the same init path. Make sctp_sysctl_net_unregister() tolerate a missing header and clear the saved pointer so init-error and exit paths can safely share the unregister helper.	2026-08-10	7.8	CVE-2026-68162

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/page_vma_mapped: fix device-private PMD handling Commit 65edfda6f3f2 ("mm/rmap: extend rmap and migration support device-private entries") introduced the concept of device-private PMD entries, but did not correctly update the rmap walk code to account for them. As a result, when page_vma_mapped_walk() encounters device-private PMD entries, it takes no action other than to acquire the PMD lock and exit. However this is highly problematic for two reasons - firstly, device private entries possess a PFN so check_pmd() needs to be called to ensure an overlapping PFN range. Secondly, and more importantly, if PVMW_MIGRATION is set the caller assumes the returned entry is a migration entry, resulting in memory corruption when the caller tries to interpret the device private entry as such. In addition, commit 146287290023 ("mm/huge_memory: implement device-private THP splitting") allowed device private PMDs to be split like THP mappings, but again did not update this code path. As a result, we might race a PMD split prior to acquiring the PMD lock. This patch addresses all of these issues by invoking check_pmd(), ensuring PVMW_MIGRATION is not set and checks whether a split raced us we do for PMD THP and migration entries. Instead of checking for a subset of the cases after taking the pmd_lock(), put device-private along with pmd_trans_huge() and pmd_is_migration_entry(). Also remove thp_migration_supported() as it is already guarded by pmd_is_migration_entry(). [akpm@linux-foundation.org: fix Raspberry Pi 1 build, per David]	2026-08-10	7.8	CVE-2026-68163
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: arm64: make huge_ptep_get handled unaligned addresses huge_ptep_get() can be handed a virtual address pointing to the middle of a contpmd/contpte mapped hugetlb folio (examples of callers are pagemap_hugetlb_range, page_mapped_in_vma). The arm64 helper rewalks the pgtables in find_num_contig to answer whether the huge pte we have maps a contpmd or a contpte hugetlb folio, and returns CONT_PMDs or CONT_PTES, so that it can collect a/d bits over the contiguous ptes. We can falsely return CONT_PTES instead of CONT_PMDs if the addr is not aligned. On systems where CONT_PTES != CONT_PMDs (meaning page size is 16K), we could collect excess A/D bit state, meaning extra work for the kernel. Even worse, we may iterate beyond the PTE table and dereference a garbage ptep pointer to access physical memory we don't own. Since the ptep pointer is a linear map address, we may run off the end of the linear map or into a hole, dereference a VA not mapped into the kernel pgtables and cause kernel panic. Fix this by aligning the pmdp pointer down to a contpmd base before checking equality with the passed huge pte pointer, to correctly answer whether the huge pte is the base of a contpmd block.	2026-08-10	7.1	CVE-2026-68172
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ublk: wait on ublk_dev_ready() instead of ub->completion ub->completion is only re-armed by a successful START_USER_RECOVERY. If the ublk server sends END_USER_RECOVERY without one - e.g. its START failed with -EBUSY and the error was ignored - the wait is satisfied by the stale completion of the previous recovery cycle, and the device is marked LIVE and the requeue list kicked while the FETCH stream is still running and ubq->canceled is still set. The kick redispatches a previously requeued request, __ublk_queue_rq_common() sees ->canceled and parks it again via __ublk_abort_rq(), and after the last FETCH clears ->canceled nothing ever kicks the requeue list again: the request is stranded there while holding its tag. If it is the flush machinery's flush_rq, every subsequent fsync piles up in uninterruptible sleep and teardown hangs on tag draining. This matches a report of a lost PREFLUSH with ext4 on top of ublk after daemon crash recovery. ub->completion is an edge-triggered latch used as a proxy for the level condition "every queue has fetched all I/O commands", which can regress (F_BATCH's UNPREP, daemon death) and whose re-arm can be skipped. Drop it and wait on the real condition instead: the new helper ublk_wait_dev_ready_and_lock() waits on ublk_dev_ready() via wait_var_event_interruptible(), woken from ublk_mark_io_ready(), then re-checks it under ub->mutex, waiting again on regression, and returns with the mutex held and readiness guaranteed. Readiness becomes true in the same ub->mutex critical section that clears the last queue's ->canceled, so END_USER_RECOVERY marks the device LIVE and kicks the requeue list strictly after ->canceled clears. The wait stays interruptible, so a server whose daemon died can still be signalled out. For ublk_ctrl_start_dev() this replaces the fail-fast -EINVAL on an F_BATCH ready->UNPREP regression with waiting until the device is ready again.	2026-08-10	7.1	CVE-2026-68173

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tracing: Delay module ref count for "enable_event" trigger Triggers are now delayed from freeing, but can still be triggered until after the RCU grace period has ended. The freeing of the enable_event data is put into the private_data_free() callback, but the put of the module refcount is done immediately. It is possible that if a module is removed that has an event that would enable (or disable) it is still active, it can read the data of the module after it is removed causing a use-after-free bug. Move the trace_event_put_ref() that releases the module into the delayed callback so that the module can not be removed until any reference to its events are finished.	2026-08-10	7.8	CVE-2026-68177
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: misc: nsm: pin the module while the device is open misc_open() installs a misc driver's file operations with fops_get(), which pins file_operations::owner before replacing the file's f_op. The NSM misc device leaves nsm_dev_fops.owner unset, so opening /dev/nsm does not take a module reference on the nsm driver. If the driver is built as a module, an open file descriptor can therefore survive rmmod of the module that provides its ioctl callbacks. A later ioctl through that descriptor can call into unloaded module text. Set nsm_dev_fops.owner to THIS_MODULE so the misc core holds the module while any /dev/nsm file descriptor is open, matching the lifetime expectation for the installed file operations.	2026-08-10	7.8	CVE-2026-68178
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: Protect UUID list traversal The hci_sync conversion moved class-of-device and EIR generation from an HCI request built under hdev->lock to asynchronous command sync work. The worker holds hdev->req_lock, but that lock does not serialize access to hdev->uuids against add_uuid() and remove_uuid(), which update the list under hdev->lock. The following interleaving can therefore occur: CPU0 (command sync work) CPU1 (management socket) fetch uuid from the list list_del(&uuid->list) kfree(uuid) read uuid->size KASAN reports the resulting use-after-free: BUG: KASAN: slab-use-after-free in eir_create+0xb8f/0xee0 Read of size 1 at addr ffff88810dbd8620 by task kworker/u17:0/87 Workqueue: hci0 hci_cmd_sync_work Call Trace: eir_create+0xb8f/0xee0 hci_update_eir_sync+0x1c0/0x330 hci_cmd_sync_work+0x13c/0x290 process_one_work+0x63a/0x1070 worker_thread+0x45b/0xd10 Allocated by task 86: __kasan_kmalloc+0x8f/0xa0 add_uuid+0x18a/0x4b0 hci_sock_sendmsg+0x1033/0x1ea0 Freed by task 92: __kasan_slab_free+0x43/0x70 kfree+0x131/0x3c0 remove_uuid+0x25e/0x560 hci_sock_sendmsg+0x1033/0x1ea0 Hold hdev->lock while generating and committing the class-of-device and EIR snapshots. Release it before sending an HCI command, so controller waits do not happen under the device lock. This protects all UUID list walks in these paths and restores the serialization lost in the command sync conversion.	2026-08-10	7.8	CVE-2026-68189
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: timer: don't re-enter an instance callback that is still running The userspace-driven timer (utimer) TRIGGER ioctl calls snd_timer_interrupt() directly with no serialization, so two threads triggering the same utimer can run snd_timer_interrupt() on one snd_timer concurrently. snd_timer_process_callbacks() drops timer->lock around each instance callback and marks the in-flight callback with the single SNDRV_TIMER_IFLG_CALLBACK bit; snd_timer_close_locked() waits on that bit to drain an in-flight callback before freeing the instance. The bit cannot represent two concurrent callbacks: when a second interrupt re-queues an instance whose callback is still running, both run at once, the first to finish clears the bit, and the close-path drain then frees the instance (and its callback_data) while the other callback is still live - a use-after-free reachable by any user able to open /dev/snd/timer, both via a user timer instance and via a sequencer queue timer bound to the utimer. snd_timer_interrupt() sets IFLG_CALLBACK before dropping timer->lock, so a concurrent interrupt already observes it under the lock. Skip re-queuing an instance (and its slaves) to the ack/sack list while its callback is in flight; the accumulated pticks are delivered on the next tick, so no event is lost.	2026-08-10	7.8	CVE-2026-68200
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: timer: drain a slave's callback before its master detaches it snd_timer_close_locked() drains the closing instance's own in-flight callback (IFLG_CALLBACK) before freeing it, but not its slaves'. When a master instance is closed, remove_slave_links() clears each slave's ->timer; the slave's own close then reads timer == NULL and takes the branch that skips the drain entirely (snd_timer_stop_slave() also no-ops on a NULL timer). So a slave whose callback is still running when the master is closed is freed underneath the live callback, leading to use-after-free. Drain the slaves too before	2026-08-10	7.8	CVE-2026-68201

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remove_slave_links() severs them. snd_timer_stop() has already taken this instance off the active list, so no new slave callback can be queued. Take the slaves off the ack list so a pending one can't fire either, then wait for any that is already in flight.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: seq: close a re-opened queue timer in the destructor queue_delete() closes the queue timer, then frees it. snd_seq_timer_close() clears q->timer->timeri. snd_use_lock_sync() then drains borrowers, and snd_seq_timer_delete() frees q->timer. A borrower can re-open the timer inside that window. A SET_QUEUE_CLIENT that took a queueptr() use_lock reference before the queue was unlinked runs snd_seq_timer_open() after the close. Open refuses re-open only while timeri is set, and the close just cleared it, so it re-opens timeri. snd_seq_timer_delete() does not close that instance. Its snd_seq_timer_stop() is a no-op, because running was cleared first. So it frees q->timer with the instance still live. The queue is freed next. The instance stays on the global timer with callback_data pointing at the freed queue. A non-owner START on the unlocked queue arms it. The next tick derefs the freed queue in snd_seq_timer_interrupt(). Reachable by an unprivileged user with access to /dev/snd/seq. No CAP and no queue ownership required. Close any lingering instance in the destructor. There, ->timeri can no longer change: the queue is unlinked and all use_lock borrowers have drained, so no snd_seq_queue_use() can re-open it. Close it before clearing q->timer. snd_timer_close() waits for any in-flight snd_seq_timer_interrupt() to finish, and that callback still reads q->timer (via snd_seq_check_queue()), so q->timer must stay valid until it drains.	2026-08-10	7.8	CVE-2026-68202
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: vivid: check for vb2_is_busy() when toggling caps The vivid_update_format_cap/out() functions must only be called if the capture/output queue are not busy. But for the controls that select the CROP/COMPOSE/SCALE capability that is not checked. Only when streaming starts will they be set to 'grabbed' and it is impossible to change the control, but between REQBUEFS and STREAMON you are still allowed to set these controls. Since vivid_update_format_cap/out will change the format, this can cause unexpected results. Besides adding these checks, also add a WARN_ON in vivid_update_format_cap/out() if the queue is busy. I'm 90% certain that this is the cause of this syzbot bug: https://syzkaller.appspot.com/bug?extid=dac8f5eaa46837e97b89 But since we never have reproducers, it is hard to be certain. In any case, these checks are needed regardless.	2026-08-10	7.8	CVE-2026-68204
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: v4l2-ctrls: validate HEVC active reference counts HEVC slice parameters are shared stateless V4L2 controls, but the common validation path does not verify the active L0/L1 reference counts before driver-specific code consumes them. The original report came from Cedrus, but the active count bounds are not Cedrus-specific. Validate them in the common HEVC slice control path so stateless HEVC drivers get the same basic guarantees as soon as the control is queued. Do not reject ref_idx_l0/ref_idx_l1 entries here. Existing userspace may use out-of-range sentinel values such as 0xff for missing references, and some hardware can use that information for concealment. Keep this common check limited to the active reference counts.	2026-08-10	7.8	CVE-2026-68206
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: sun4i-csi: Return queued buffers on start_streaming() failure The vb2 framework hands buffers to the driver via buf_queue() before calling start_streaming(). If start_streaming() returns an error without first returning those buffers via vb2_buffer_done(), vb2_start_streaming() fires WARN_ON(owned_by_drv_count) and the queued buffers leak. sun4i_csi_start_streaming() returned -EINVAL when no matching CSI format could be found, before any setup (scratch buffer allocation, pipeline start) had been performed. The remaining error paths already converge on the err_clear_dma_queue label, which calls return_all_buffers(..., VB2_BUF_STATE_QUEUED) under csi->qlock. Jump to that label directly: the intermediate err_disable_device / err_disable_pipeline / err_free_scratch_buffer labels are skipped, which is correct because nothing they would undo has happened yet. This mirrors the uvcvideo fix in commit 4cf3b6fd54eb ("media: uvcvideo: Return queued buffers on start_streaming() failure").	2026-08-10	7.8	CVE-2026-68209
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: stm32: dcmi: unregister notifier on probe failure dcmi_graph_init() registers the async notifier before dcmi_probe() toggles the reset line. If reset_control_assert() or	2026-08-10	7.8	CVE-2026-68210

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	reset_control_deassert() fails afterwards, probe returns through err_cleanup and the driver core will not call dcmi_remove(). Unregister the notifier before cleaning it up on that error path, matching the successful remove path and the V4L2 async notifier lifetime rules. [hverkuil: added Fixes tag]			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: rtl2832_sdr: Return queued buffers on start_streaming() failure The vb2 framework hands buffers to the driver via buf_queue() before calling start_streaming(). If start_streaming() returns an error without first returning those buffers via vb2_buffer_done(), vb2_start_streaming() fires WARN_ON(owned_by_drv_count) and the queued buffers leak. rtl2832_sdr_start_streaming() had multiple error paths that hit this trap: two direct early returns (-ENODEV, -ERESTARTSYS), plus six `goto err` paths covering subdev s_power, tuner setup, ADC setup, stream-buffer allocation, urb allocation, and urb submission failures. None of them returned the queued buffers. The original function had no distinct success exit and fell straight through into the err label, which previously only did mutex_unlock and "return ret". Adding queued-buffer cleanup at err must therefore be paired with an explicit success return; otherwise every successful start would also drain the buffer queue and kill streaming. Add that success return, then add rtl2832_sdr_cleanup_queued_bufs() at the err label and before each early return. The cleanup helper takes a vb2_buffer_state argument so that the start_streaming error paths can pass VB2_BUF_STATE_QUEUED (as expected by userspace on start_streaming failure) while stop_streaming keeps its existing VB2_BUF_STATE_ERROR semantics. This mirrors the uvcvideo fix in commit 4cf3b6fd54eb ("media: uvcvideo: Return queued buffers on start_streaming() failure"). The err label still does not roll back power_ctrl(), frontend_ctrl(), the POWER_ON flag, or stream/URB allocations that may have happened before the failing step. Those are pre-existing leaks of a different class and are not addressed here.	2026-08-10	7.8	CVE-2026-68213
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: pwc: Return queued buffers on start_streaming() failure The vb2 framework hands buffers to the driver via buf_queue() before calling start_streaming(). If start_streaming() returns an error without first returning those buffers via vb2_buffer_done(), vb2_start_streaming() fires WARN_ON(owned_by_drv_count) and the queued buffers leak. pwc's start_streaming() had two early returns that hit this trap: -ENODEV when the USB device was already disconnected, and -ERESTARTSYS when mutex_lock_interruptible() was interrupted by a signal. Call the existing pwc_cleanup_queued_bufs() helper with VB2_BUF_STATE_QUEUED before returning (matching the state already used by the pwc_isoc_init() error path in the same function). This mirrors the uvcvideo fix in commit 4cf3b6fd54eb ("media: uvcvideo: Return queued buffers on start_streaming() failure").	2026-08-10	7.8	CVE-2026-68216
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: nxp: imx8-isi: Fix potential out-of-bounds issues The maximum downscaling factor supported by ISI can be up to 16. Add minimum value constraint before applying the setting to hardware. Otherwise, the process will not respond even when Ctrl+C is executed.	2026-08-10	7.8	CVE-2026-68219
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: msi2500: Return queued buffers on start_streaming() failure The vb2 framework hands buffers to the driver via buf_queue() before calling start_streaming(). If start_streaming() returns an error without first returning those buffers via vb2_buffer_done(), vb2_start_streaming() fires WARN_ON(owned_by_drv_count) and the queued buffers leak. msi2500_start_streaming() had five error paths that all hit this trap and were further tangled by ret-overwriting between calls: - - ENODEV when the USB device was already disconnected - -ERESTARTSYS when mutex_lock_interruptible() was interrupted - msi2500_set_usb_adc() failure: ret was silently overwritten by the next call (msi2500_isoc_init()), so the error was lost entirely - msi2500_isoc_init() failure: cleanup_queued_bufs was called, but the function then fell through to msi2500_ctrl_msg() and again masked the original error by overwriting ret - msi2500_ctrl_msg(CMD_START_STREAMING) failure: no cleanup at all, leaving isoc URBs submitted with no way for the driver to consume them Consolidate the error paths into a small goto chain. Every failure now stops the function, drains the queued-buffer list, and returns the real error code. The ctrl_msg failure path also rolls back the preceding msi2500_isoc_init() via msi2500_isoc_cleanup() before unlocking and draining. The cleanup helper takes a vb2_buffer_state argument so that the start_streaming error paths can pass VB2_BUF_STATE_QUEUED (as expected by userspace on start_streaming failure)	2026-08-10	7.8	CVE-2026-68222

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	while stop_streaming keeps its existing VB2_BUF_STATE_ERROR semantics. This mirrors the uvcvideo fix in commit 4cf3b6fd54eb ("media: uvcvideo: Return queued buffers on start_streaming() failure").			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: chips-media: wave5: Move src_buf Removal to finish_encode During encoder processing, there is a case where the IRQ response could return the buffer back to userspace via v4l2_m2m_buf_done call. In this time, userspace could queue up this same buffer before start_encode removes the index from the ready queue. This would then lead to a case where the buffer in the ready queue could be a self loop due to the WRITE_ONCE(prev->next, new) call in __list_add. When __list_del is finally called, the loop is already made so nothing points back to ready queue list head and pointers are poisoned. A buffer should not be marked as DONE before the buffer is removed from m2m ready queue. Move removal entirely to finish_encode.	2026-08-10	7.8	CVE-2026-68228
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: cedrus: skip invalid H.264 reference list entries Cedrus consumes H.264 ref_pic_list0/ref_pic_list1 entries from the stateless slice control and later uses their indices to look up decode->dpb[] in _cedrus_write_ref_list(). Rejecting such controls in cedrus_try_ctrl() would break existing userspace, since stateless H.264 reference lists may legitimately carry out-of-range indices for missing references. Instead, guard the actual DPB lookup in Cedrus and skip entries whose indices do not fit the fixed V4L2_H264_NUM_DPB_ENTRIES array. This keeps the fix local to the driver use site and avoids out-of-bounds reads from malformed or unsupported reference list entries.	2026-08-10	7.1	CVE-2026-68229
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: amlogic-c3: Add validations for ae and awb config Avoid invalid memory access if the zones_num is bigger than zone_weight. This patch fixes the following smatch errors: drivers/media/platform/amlogic/c3/isp/c3-isp-params.c:111 c3_isp_params_awb_wt() error: buffer overflow 'cfg->zone_weight' 768 <= u32max drivers/media/platform/amlogic/c3/isp/c3-isp-params.c:111 c3_isp_params_awb_wt() error: buffer overflow 'cfg->zone_weight' 768 <= u32max drivers/media/platform/amlogic/c3/isp/c3-isp-params.c:227 c3_isp_params_ae_wt() error: buffer overflow 'cfg->zone_weight' 255 <= u32max drivers/media/platform/amlogic/c3/isp/c3-isp-params.c:227 c3_isp_params_ae_wt() error: buffer overflow 'cfg->zone_weight' 255 <= u32max	2026-08-10	7.3	CVE-2026-68230
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: set new_stream to NULL after release In dm_update_crtc_state(), the skip_modeset path releases new_stream via dc_stream_release() but does not set the pointer to NULL. If a later error (e.g., color management failure) triggers the fail label, the error path calls dc_stream_release() again on the same dangling pointer, causing a double release and potential use-after-free. Fix this by setting new_stream to NULL after the initial release. (cherry picked from commit 99f3af19073b3ddb96e789124cce12c4277b28)	2026-08-10	7.8	CVE-2026-68236
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix lifetime issue of amdgpu_vm_get_task_info_pasid() The vm pointer returned from amdgpu_vm_get_vm_from_pasid() is only valid while the lock is still being held. Once xa_unlock_irqrestore is called and returned, the pointer is no longer under lock and is subject to modification. Since, the caller still dereferences vm->task_info in amdgpu_vm_get_task_info_vm() after the lock is removed, this causes a use after unlock problem. Remove the lifetime issue present in amdgpu_vm_get_task_info_pasid() through removing the amdgpu_vm_get_vm_from_pasid() function from amdgpu_vm.c and making the relevant code inline to hold the lock while it is still in use. (cherry picked from commit 9d01579f3f868b333acc901815972685989092c7)	2026-08-10	7.8	CVE-2026-68245
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/i915/hdcp: check streams[] bounds before overflow The data->streams[] overflow check is done after the buffer overflow has already happened. Move the overflow check before the write. Side note, emitting a warning splat with a backtrace might be overkill here, but prefer not changing the behaviour other than not doing the overrun. Discovered using AI-assisted static analysis confirmed by Intel Product Security. (cherry picked from commit 9284ab3b6e776c315883ac2611283d263c9460fd)	2026-08-10	7.8	CVE-2026-68253

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/virtio: bound EDID block reads to the response buffer virtio_get_edid_block() validates the read offset only against the device-supplied resp->size field, never against the fixed-size resp->edid array. The EDID block index is driven by the device-supplied extension count, so a malicious virtio-gpu backend can advertise a large size together with a high block count and read far past the array into adjacent kernel memory, which is then surfaced in the parsed EDID (an out-of-bounds read / info leak). Also reject any read whose end exceeds the size of the edid array. Conforming EDID responses stay within the array and are unaffected.	2026-08-10	7.7	CVE-2026-68255
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: fix 32-bit overflow in CWSR total size calculation total_cwsr_size was computed in 32-bit before being used as a BO/SVM allocation size. With large ctx_save_restore_area_size and debug_memory_size multiplied by the XCC count, the product can wrap, yielding an undersized CWSR save area that firmware later overruns. Promote total_cwsr_size to u64 and use check_add_overflow()/check_mul_overflow() in both kfd_queue_acquire_buffers() and kfd_queue_release_buffers(). (cherry picked from commit 319f7e13423ae3f486b9aea82f9ad2d6af0ee608)	2026-08-10	7.8	CVE-2026-68257
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Check bounds on CRIU restore queue type and mqd size We weren't checking whether the values provided in the private data in kfd CRIU restore were within bounds. For queue type, add a KFD_QUEUE_TYPE_MAX and ensure the provided type is less than it. For mqd_size, add new function mqd_size_from_queue_type and confirm that the provided mqd_size matches expectations. (cherry picked from commit f19d8086f6644083c913d70bfdeee20e1b6f46a5)	2026-08-10	7.1	CVE-2026-68258
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: acquire vm_ctx->lock before mapping memory to GPU VM The drm gpuvmm code doesn't protect find operation against map operation, and the driver needs to ensure a map operation shouldn't happen when a find operation is in progress. In some cases a find operation will be in progress when doing map/unmap operations, and the find operation will do a NULL pointer dereference. An example of the stack trace of such NULL dereference is shown below: `` Unable to handle kernel access to user memory without uaccess routines at virtual address 0000000000000010 [<ffffff01e989d4>] drm_gpuva_find+0x28/0x6c [drm_gpuvm] [<ffffff01ed3a40>] pvr_vm_unmap+0x34/0x68 [powervr] [<ffffff01ec69da>] pvr_ioctl_vm_unmap+0x2e/0x50 [powervr] [<ffffff8080ce0a>] drm_ioctl_kernel+0x8e/0xdc [<ffffff8080d016>] drm_ioctl+0x1be/0x3e0 [<ffffff802bec3e>] __riscv_sys_ioctl+0xba/0xc4 [<ffffff80d858b2>] do_trap_ecall_u+0x23e/0x3f4 [<ffffff80d92288>] handle_exception+0x168/0x174 `` As all occurrences of drm_gpuva_find*() are already guarded by vm_ctx->lock, make pvr_vm_map() to acquire this lock to prevent disturbing any find operation. This fixes the NULL deference problem in drm_gpuva_find*().	2026-08-10	7.8	CVE-2026-68260
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Fix user array stride in pvr_set_uobj_array() pvr_set_uobj_array() copies an array of kernel objects to a userspace array whose element size is described by out->stride. When out->stride is different from the kernel object size, the slow path advances the userspace pointer by the kernel object size and the kernel pointer by the userspace stride. This reverses the intended layout. For larger userspace strides, later copies read from the wrong kernel addresses. For smaller userspace strides, later copies are written at the wrong userspace offsets. The padding clear is also done only for the first element instead of the padding area for each element. Advance the userspace pointer by out->stride and the kernel pointer by obj_size, and clear per-element padding while the current userspace pointer is still available.	2026-08-10	7.1	CVE-2026-68262
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Fix double call to drm_sched_entity_fini() Call sequence of double call: pvr_context_destroy fpvr_context_kill_queues fpvr_queue_kill drm_sched_entity_destroy fdrm_sched_entity_fini // here pvr_context_put kref_put(..., pvr_context_release) pvr_context_destroy_queues pvr_queue_destroy drm_sched_entity_fini // here Call to drm_sched_entity_destroy() from pvr_context_kill_queues() calls drm_sched_entity_flush() + drm_sched_entity_fini(). drm_sched_entity_flush() ensures all pending jobs are completed and drm_sched_entity_fini() ensures no further submission is allowed as per expectation from pvr_context_kill_queues(). Double call to drm_sched_entity_fini() is misuse of the API so keep call only in	2026-08-10	7.8	CVE-2026-68263

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pvr_context_create() failure path. Stack trace for issue with addition of refcounting for DRM entity stats in commit fd177135f0e6 ("drm/sched: Account entity GPU time"): [789.490527] -----[cut here]----- [789.490559] refcount_t: underflow; use-after-free. [789.490657] WARNING: lib/refcount.c:28 at refcount_warn_saturate+0xf4/0x144, CPU#0: kworker/u16:1/440 [789.490695] Modules linked in: powervr drm_gpuvm drm_exec gpu_sched drm_shmem_helper xhci_plat_hcd xhci_hcd dwc3 usbcore usb_common snd_soc_simple_card snd_soc_simple_card_utils sa2ul sha512 sha256 dwc3_am62 sha1 authenc rti_wdt libsha512 at24 sch_fq_codel fuse dm_mod ipv6 [789.490798] CPU: 0 UID: 0 PID: 440 Comm: kworker/u16:1 Not tainted 7.0.0-rc7-02049-g5e2c0700091b #22 PREEMPT [789.490809] Hardware name: Texas Instruments AM625 SK (DT) [789.490815] Workqueue: powervr-sched pvr_queue_fence_release_work [powervr] [789.490868] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYP=--) [789.490876] pc : refcount_warn_saturate+0xf4/0x144 [789.490884] lr : refcount_warn_saturate+0xf4/0x144 [789.490892] sp : ffff8000822cbcc0 [789.490895] x29: ffff8000822cbcc0 x28: 0000000000000000 x27: 0000000000000000 [789.490909] x26: 0000000000000000 x25: ffff800081b1e338 x24: ffff000004541405 [789.490922] x23: ffff000004bea950 x22: ffff00000042e400 x21: ffff000007123e30 [789.490935] x20: ffff000007123000 x19: ffff000007a80d50 x18: ffffffff7768 [789.490948] x17: 74736574202c6e6f x16: 697461746e656d65 x15: ffff800081b269f0 [789.490962] x14: 0000000000000030 x13: ffff800081b26a70 x12: 0000000000000211 [789.490975] x11: 00000000000000c0 x10: 0000000000000b50 x9 : ffff8000822cbb30 [789.490988] x8 : ffff0000014e7bb0 x7 : ffff000007725e780 x6 : 0000000372a05f49 [789.491001] x5 : 0000000000000000 x4 : 0000000000000001 x3 : 0000000000000010 [789.491013] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0000014e7000 [789.491027] Call trace: [789.491032] refcount_warn_saturate+0xf4/0x144 (P) [789.491043] drm_sched_entity_fini+0x164/0x18c [gpu_sched] [789.491081] pvr_queue_destroy+0x64/0x134 [powervr] [789.491110] pvr_context_destroy_queues+0x34/0x64 [powervr] [789.491138] pvr_context_release+0x70/0xac [powervr] [789.491166] pvr_context_put.part.0+0x5c/0x7c [powervr] [789.491193] pvr_context_put+0x14/0x24 [powervr] [789.491221] pvr_queue_fence_release_work+0x20/0x38 [powervr] [789.491249] process_one_work+0x160/0x4c4 [789.491264] worker_thread+0x188/0x310 [789.491276] kthread+0x130/0x13c [789.491287] ret_from_fork+0x10/0x20 [789.491300] ---[end trace 0000000000000000]---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/pt: Reset current_op in xe_pt_update_ops_init() xe_pt_update_ops_init() fails to reset current_op to 0. On the vm_bind path, ops_execute() calls xe_pt_update_ops_prepare() inside the xe_validation_guard() / drm_exec_until_all_locked() loop. When that loop retries due to lock contention or OOM eviction (drm_exec_retry_on_contention() / xe_validation_retry_on_oom()), xe_pt_update_ops_prepare() runs again on the same vops, and each call to bind_op_prepare() increments current_op without resetting it. After N retries current_op exceeds the array size allocated by xe_vma_ops_alloc(), causing an out-of-bounds write into SLUB-poisoned memory and a subsequent UAF crash in xe_migrate_update_ptables_cpu() when reading the corrupted pt_op->bind. Also reset needs_svm_lock and needs_invalidation which are derived in the same prepare pass and would otherwise cause wrong migrate ops selection and redundant TLB invalidation on retry. Fix this by resetting current_op, needs_svm_lock and needs_invalidation in xe_pt_update_ops_init(). v2 (Matt): - Add details in commit message. - Add Fixes tag and Cc to stable@vger.kernel.org (cherry picked from commit 046045543e530605c441063535e7dca0075369a6)	2026-08-10	7.8	CVE-2026-68264
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/vm: Fix BO prefetch with CONSULT_MEM_ADVISE_PREF_LOC When prefetch region is DRM_XE_CONSULT_MEM_ADVISE_PREF_LOC for a BO VMA, the code used it as an index into region_to_mem_type[], causing an out-of-bounds access since the value is -1. Resolve the preferred location for BO VMAs directly: local VRAM on dGFX (using the BO's tile placement) or system memory on iGPU. Discovered using AI-assisted static analysis confirmed by Intel Product Security. v2: -Fix null dereference (cherry picked from commit d9a4906ac03be9f6ed3f3b45c56c866b867fd75b)	2026-08-10	7.3	CVE-2026-68265

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Hold a dma-buf reference for imported BOs An imported dma-buf BO is created as a ttm_bo_type_sg BO whose reservation object is the exporter's dma_buf->resv. The importer, however, only takes a dma-buf reference after a successful dma_buf_dynamic_attach(). Until then nothing keeps the exporter alive, so if the exporter is freed while the BO still references its resv, a later access to that resv is a use-after-free: Oops: general protection fault, probably for non-canonical address 0x6b6b6b6b6b6b6b9c Workqueue: ttm ttm_bo_delayed_delete [ttm] RIP: 0010:mutex_can_spin_on_owner+0x3f/0xc0 This can be reached on two paths: - dma_buf_dynamic_attach() fails, or - ttm_bo_init_reserved() fails during BO creation. In both cases the BO already has bo->base.resv pointing at the exporter resv, and sg BOs are always torn down via ttm_bo_delayed_delete(), which locks bo->base.resv asynchronously - potentially after the exporter has been freed. Take the dma-buf reference in xe_bo_init_locked(), before ttm_bo_init_reserved(), so it also covers a creation failure there, and release it in xe_ttm_bo_destroy(). The reference is held for the whole BO lifetime, keeping the shared resv alive on every path. v2: - Reworked the fix to avoid creating the imported sg BO before dma_buf_dynamic_attach() succeeds. - Attach with importer_priv == NULL and make invalidate_mappings ignore incomplete imports. v3: - Dropped the xe-side reordering approach since importer_priv must be valid when dma_buf_dynamic_attach() publishes the attachment. - Per Christian's suggestion on the v1 thread, keyed the check on import_attach rather than removing the sg guard entirely. - Fixes both xe and amdgpu in a single TTM patch. v4: - Moved import_attach check to after dma_resv_copy_fences() so fences are copied before returning for successful imports (Thomas). - Removed exporter-alive claim from commit message (Thomas). v5: - Add drm/xe patch to keep imported sg BOs off the LRU before attach succeeds; the TTM fix alone is not sufficient for xe if the BO is already LRU-visible. (Thomas) v4 patch: https://patchwork.freedesktop.org/patch/736663/?series=169129&rev=2 - Patch 1 (drm/ttm) carries Christian's Reviewed-by from v4. v6: - Reworked the fix based on Thomas' suggestion. Instead of the TTM resv individualization (v1-v5) plus the xe off-LRU/placement handling (v5), just hold a dma-buf reference for the imported BO lifetime so the shared resv can never be freed while the BO still references it. Single xe patch, no TTM change. (Thomas) - Take the reference in xe_bo_init_locked() before ttm_bo_init_reserved() so a TTM creation failure is covered too (Thomas). - Dropped the v5 series (drm/ttm + drm/xe off-LRU); the off-LRU approach also regressed in CI BAT via ttm_bo_pipeline_gutting() creating a ghost BO that outlived the exporter. Link to v5: https://patchwork.freedesktop.org/series/169984/ v7: - Move changelog above --- so it stays in the commit message. - Reorder changelog entries oldest-to-newest. (Thomas) (cherry picked from commit 3516f3fae6be35642f8f06f8a218da6425c0306a)	2026-08-10	7.8	CVE-2026-68266
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix context pstate override handling There are several problems in the context pstate handling code. The most serious ones are potential use-after-free and NULL pointer dereferences at context initialization time. Both are due amdgpu_ctx_init() not holding the adev->pm.stable_pstate_ctx_lock, which is otherwise used from both sysfs and the context code itself for modifying and clearing the stored context pointer. Second issue is that context fini can trample over the pstate configuration set via sysfs. This is due the restore state (ctx->stable_pstate) being saved at context init time, and not if, or when the context actually changes the pstate. As the context exits it will therefore incorrectly restore to what was set before the sysfs override was requested. The simplest fix is to drastically simplify how the state is tracked, by clearly defining the points at which pstate ownership is taken and released, and to handle all transitions under the correct lock. Instead of at context init time, the previous state is saved only at the point the context overrides the current state, and is restored on context exit only if the context is still the owner of the current override state. (cherry picked from commit 1b5e413713c0a93bc1818394d0ce49aad21bd27)	2026-08-10	7.8	CVE-2026-68273
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/guc: Fix buffer overflow in steered register list allocation The size calculation for the steered register extarray uses only the geometry DSS mask (g_dss_mask) to determine the number of entries to allocate: total = bitmap_weight(gt->fuse_topo.g_dss_mask, ...) * steer_reg_num; However, the filling loop uses for_each_dss_steering(), which iterates over for_each_dss(), defined as the union	2026-08-10	7.8	CVE-2026-68274

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of g_dss_mask and c_dss_mask (geometry + compute DSS). On platforms with compute-only DSS bits, the loop writes past the allocated buffer, corrupting adjacent slab objects. This manifests as list_del corruption and SLUB redzone overwrites during drm_managed_release on device unbind, since the overflow corrupts the drmres list_head of neighboring allocations. Fix by computing the allocation size using the union of both DSS masks, matching the iteration pattern of for_each_dss_steering(). -- v2: - use bitmap_weighted_or() (Zhanjun) (cherry picked from commit 0a78a44f4901aa6c9263e66be7fce02282f1109f)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf, sockmap: Fix cork use-after-free in tcp_bpf_sendmsg() tcp_bpf_sendmsg() keeps msg_tx across sk_stream_wait_memory(), which drops and reacquires the socket lock. Its error path tries to decide whether msg_tx names the local temporary message by comparing it with the current value of psock->cork. This comparison is unsafe when two threads send on the same socket: Thread A Thread B msg_tx = psock->cork sk_msg_alloc() fails sk_stream_wait_memory() releases the socket lock acquires the socket lock completes the cork psock->cork = NULL frees the cork reacquires the socket lock msg_tx != psock->cork sk_msg_free(msg_tx) The stale cork is therefore mistaken for the local temporary message and freed again. KASAN reported: BUG: KASAN: slab-use-after-free in sk_msg_free+0x49/0x50 Read of size 4 at addr ffff88810c908800 by task poc/90 Call Trace: sk_msg_free+0x49/0x50 tcp_bpf_sendmsg+0x14f5/0x1cc0 __sys_sendto+0x32c/0x3a0 __x64_sys_sendto+0xdb/0x1b0 Allocated by task 89: __kasan_kmalloc+0x8f/0xa0 tcp_bpf_sendmsg+0x16b3/0x1cc0 Freed by task 91: __kasan_slab_free+0x43/0x70 kfree+0x131/0x3c0 tcp_bpf_sendmsg+0xec3/0x1cc0 msg_tx can only name the stack-local tmp or the shared cork. Check for tmp directly so a changed psock->cork cannot turn a shared message into an apparent local one.	2026-08-10	7.8	CVE-2026-68284
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drop_monitor: fix size calculations for 64-bit attributes net_dm_packet_report_fill() and net_dm_hw_packet_report_fill() use nla_put_u64_64bit() to append 64-bit attributes (NET_DM_ATTR_PC and NET_DM_ATTR_TIMESTAMP). On 32-bit architectures without CONFIG_HAVE_EFFICIENT_UNALIGNED_ACCESS, nla_put_u64_64bit() may append a 4-byte NET_DM_ATTR_PAD attribute for 64-bit alignment. However, net_dm_packet_report_size() and net_dm_hw_packet_report_size() used nla_total_size(sizeof(u64)) instead of nla_total_size_64bit(sizeof(u64)), budgeting 12 bytes instead of up to 16 bytes. This under-estimation of SKB size can lead to an skb_over_panic() when __nla_reserve() or skb_put() is subsequently called. Fix this by using nla_total_size_64bit(sizeof(u64)) in both size calculations.	2026-08-10	7.5	CVE-2026-68287
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rds: tcp: unregister sysctl before tearing down listen socket rds_tcp_exit_net() frees the per-netns RDS TCP listen socket via rds_tcp_kill_sock() before unregistering the per-netns sysctl table. Since rds_tcp_skbuf_handler() derives the netns from rtn->rds_tcp_listen_sock->sk, a concurrent sysctl write can race with netns teardown and dereference the freed socket/sk. KASAN reports the race as: BUG: KASAN: slab-use-after-free in rds_tcp_skbuf_handler+0x2aa/0x2e0 rds_tcp_skbuf_handler net/rds/tcp.c:721 proc_sys_call_handler fs/proc/proc_sysctl.c vfs_write fs/read_write.c __x64_sys_pwrite64 fs/read_write.c Fix this by unregistering the RDS TCP sysctl table before calling rds_tcp_kill_sock(). unregister_net_sysctl_table() prevents new sysctl handlers from starting and waits for in-flight handlers to finish, so the listen socket can then be released safely. The fix was tested against the linked reproducer.	2026-08-10	7.8	CVE-2026-68290
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix MCIA register buffer overflow on 32 dword reads The MCIA register can return up to 32 dwords (128 bytes) when the device advertises the mcia_32dwords capability, but struct mlx5_ifc_mcia_reg_bits only defines dword_0..11, leaving room for just 12 dwords (48 bytes) of data. mlx5_query_mcia() clamps the read size to mlx5_mcia_max_bytes() and then memcpy()s that many bytes out of the register, potentially reading past the end of the 'out' buffer. On kernels built with FORTIFY_SOURCE this is caught as a buffer overflow while reading the module EEPROM via ethtool: detected buffer overflow in memcpy kernel BUG at lib/string_helpers.c:1048! RIP: 0010:fortify_panic+0x13/0x20 Call Trace: mlx5_query_mcia.isra.0+0x200/0x210 [mlx5_core] mlx5_query_module_eeprom_by_page+0x4a/0xa0 [mlx5_core] mlx5e_get_module_eeprom_by_page+0xbb/0x120 [mlx5_core]	2026-08-10	7.1	CVE-2026-68293

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	eeeprom_prepare_data+0xf3/0x170 ethnl_default_doit+0xf1/0x3b0 Extend the mcia_reg layout to 32 dwords.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: LoongArch: BPF: Zero-extend signed ALU32 div/mod results ALU32 operations write a 32-bit result and leave the upper 32 bits of the BPF register zero. The LoongArch JIT sign-extends the result of signed ALU32 BPF_DIV and BPF_MOD (off=1), so a negative 32-bit quotient or remainder leaves bits 63:32 set in JITted code while the verifier and interpreter model those bits as zero. Keep sign-extension on the operands, which signed divide needs, and zero-extend the ALU32 result after the divide or modulo instruction, matching the unsigned ALU32 div/mod paths and every other ALU32 operation in this JIT.	2026-08-10	7.8	CVE-2026-68295
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: fix u16 MTU truncation in media and bearer MTU validation Both TIPC_NL_MEDIA_SET and TIPC_NL_BEARER_SET accept user-supplied MTU values but only enforce a minimum bound, not a maximum. When a user sets the MTU to a value exceeding U16_MAX (65535), it passes validation but is silently truncated when assigned to u16 fields l->mtu and l->advertised_mtu in tipc_link_create(). Values like 65536 (0x10000) truncate to 0, causing a division by zero in tipc_link_set_queue_limits() which computes TIPC_MAX_PUBL / (l->mtu / ITEM_SIZE). Other overflowing values (e.g. 65537-131071) produce small incorrect MTU values, resulting in link malfunction behaviors. Crash stack (triggered as unprivileged user via user namespace): tipc_link_set_queue_limits net/tipc/link.c:2531 tipc_link_create net/tipc/link.c:520 tipc_node_check_dest net/tipc/node.c:1279 tipc_disc_rcv net/tipc/discover.c:252 tipc_rcv net/tipc/node.c:2129 tipc_udp_rcv net/tipc/udp_media.c:392 Two independent paths lack the upper bound check: 1. tipc_udp_mtu_bad() -- called from __tipc_nl_media_set() (MEDIA_SET) 2. inline check in __tipc_nl_bearer_set() at bearer.c:1160 (BEARER_SET) Fix both by rejecting MTU values above U16_MAX.	2026-08-10	7.8	CVE-2026-68297
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/vm: Fix SVM leak on resv obj alloc failure in xe_vm_create() Commit 9e9787414882 ("drm/xe/userprtr: replace xe_hmm with gpusvm") made xe_svm_init() unconditional in xe_vm_create() and extended it to also initialize a "simple" gpusvm state for non-fault-mode VMs. The matching xe_svm_fini() call in xe_vm_close_and_put() was updated to run unconditionally, but the error unwind path in xe_vm_create() was not. On the drm_gpusvm_resv_object_alloc() failure path, xe_svm_init() has already succeeded but xe_svm_fini() is only called when XE_VM_FLAG_FAULT_MODE is set. For non-fault-mode VMs this leaves vm->svm.gpusvm partially initialized and leaks the resources allocated by drm_gpusvm_init(). For fault-mode VMs, xe_svm_init() additionally acquires the pagemap owner via drm_pagemap_acquire_owner() and the pagemaps via xe_svm_get_pagemaps(). Those resources are released by xe_svm_close(), not xe_svm_fini(). On the same error path, xe_svm_close() is not called either, so fault-mode VMs leak the pagemap owner and pagemaps. Fix both leaks: - Call xe_svm_fini() unconditionally on the err_svm_fini path, matching the unconditional xe_svm_init() call. Move the vm->size = 0 assignment out of the conditional so the xe_vm_is_closed() assert in xe_svm_fini() (and xe_svm_close()) holds for both modes. - Call xe_svm_close() for fault-mode VMs before xe_svm_fini(), matching the ordering used in xe_vm_close_and_put(). (cherry picked from commit ca2a3587d577ba764e0fe628fb676244fc33ddd4)	2026-08-10	7.8	CVE-2026-68298
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vmxnet3: fix BUG_ON in vmxnet3_get_hdr_len() for Geneve packets vmxnet3_get_hdr_len() assumes gdesc->rcd.v4/v6/tcp always describe the outer header, but for a Geneve-encapsulated packet the device can set them based on the inner header instead, signalled by the VMXNET3_RCD_HDR_INNER_SHIFT bit in the completion descriptor. Since the function never skips the outer encapsulation, this mismatch triggers: - BUG_ON(hdr.ipv4->protocol != IPPROTO_TCP), because the outer protocol is UDP (Geneve), not TCP. - BUG_ON(hdr.eth->h_proto != ...), when the tunnel's outer and inner IP versions differ (e.g. outer IPv6/inner IPv4 or vice versa). Check VMXNET3_RCD_HDR_INNER_SHIFT up front and bail out, since the function cannot locate the inner header it would need to parse. Also convert the remaining BUG_ON()s in this function to return 0 defensively.	2026-08-10	7.5	CVE-2026-68299
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/vf: Add drm_dev guards when detaching CCS read/write buffers CCS read/write buffers are freed during BO destruction. In some cases, BOs may be destroyed after the device is unbound but while the DRM structure remains valid, leading to NULL pointer	2026-08-10	7.8	CVE-2026-68305

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	dereferences when accessing device resources. BUG: kernel NULL pointer dereference, address: 0000000000000000 PGD 0 P4D 0 Oops: Oops: 0000 [#1] SMP NOPTI CPU: 0 UID: 0 PID: 9376 Comm: xe_pat Not tainted 7.2.0-rc2+ #1 PREEMPT(lazy) RIP: 0010:xe_sriov_vf_ccs_rw_update_bb_addr+0x4d/0xa0 [xe] RSP: 0018:ffffcf304110b9c8 EFLAGS: 00010246 RAX: ffff8a85c38a0a00 RBX: 00000000810ef000 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffff8a85c39c1888 RBP: ffffcf304110b9e8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffff8a85c39c1888 R13: 0000000000000000 R14: ffff8a85c39b4f28 R15: ffff8a85c3885000 FS: 0000000000000000(0000) GS:ffff8a878b809000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 0000000010314a002 CR4: 0000000000772ef0 PKRU: 55555554 Call Trace: <TASK> xe_migrate_ccs_rw_copy_clear+0x98/0x120 [xe] xe_sriov_vf_ccs_detach_bo+0x2c/0x60 [xe] xe_ttm_bo_delete_mem_notify+0xc8/0xe0 [xe] ttm_bo_cleanup_memtype_use+0x26/0x80 [ttm] ttm_bo_release+0x29e/0x2d0 [ttm] ttm_bo_fini+0x39/0x70 [ttm] xe_gem_object_free+0x1f/0x30 [xe] drm_gem_object_free+0x1d/0x40 ttm_bo_vm_close+0x5f/0x90 [ttm] remove_vma+0x2c/0x70 tear_down_vmas+0x63/0xf0 exit_mmap+0x20d/0x3f0 __mmap+0x45/0x170 mmpu+0x31/0x40 do_exit+0x2ba/0xac0 do_group_exit+0x2d/0xb0 __x64_sys_exit_group+0x18/0x20 x64_sys_call+0x14a0/0x2390 do_syscall_64+0xdd/0x640 ? count_memcg_events+0xea/0x240 ? handle_mm_fault+0x1ec/0x2f0 (cherry picked from commit 1ae415a6eefe5004954a1d352b1718faca8844ef)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mctp i3c: clean up notifier and buses if driver register fails mctp_i3c_mod_init() registers the I3C bus notifier and then walks the existing buses with i3c_for_each_bus_locked(mctp_i3c_bus_add_new, NULL) before registering the I3C device driver. If i3c_driver_register() fails, the function returns the error directly, leaving the notifier registered and every mctp_i3c_bus object created for the existing buses allocated. The notifier is left pointing into the module that failed to load and the bus list is leaked. Mirror the module exit path on this failure: unregister the notifier and tear down the buses that were added before returning the error. This issue was identified during our ongoing static-analysis research while reviewing kernel code.	2026-08-10	7.8	CVE-2026-68314
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: validate stream count in sctp_process_strreset_inreq() When processing a RESET_IN_REQUEST from a peer, sctp_process_strreset_inreq() derives the stream count from the parameter length but does not check whether the resulting RESET_OUT_REQUEST would exceed SCTP_MAX_CHUNK_LEN. The OUT request header (sctp_strreset_outreq, 16 bytes) is 8 bytes larger than the IN request header (sctp_strreset_inreq, 8 bytes). Generally, the IP payload is bounded to 65535 bytes, so the stream list cannot be large enough to trigger the overflow. However, on interfaces with MTU > 65535 (e.g., loopback with IPv6 jumbograms), a stream list that fits within the incoming IN parameter can cause a __u16 overflow in sctp_make_strreset_req() when computing the OUT request size, leading to an undersized skb allocation and a kernel BUG: net/core/skbuff.c:207 skb_panic net/core/skbuff.c:2625 skb_put net/sctp/sm_make_chunk.c:1535 sctp_addto_chunk net/sctp/sm_make_chunk.c:3695 sctp_make_strreset_req net/sctp/stream.c:655 sctp_process_strreset_inreq The local setsockopt path validates the generated reset request size. However, for an incoming-only reset, it accounts for the smaller IN request even though the peer must generate an OUT request with the same stream list. Such a request cannot be completed successfully by the peer. Reject peer IN requests whose corresponding OUT request would exceed SCTP_MAX_CHUNK_LEN. Also tighten the local check so it does not send an IN request that would require an oversized OUT request from the peer.	2026-08-10	7.5	CVE-2026-68315
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel: ethosu: Fix element size accounting for cmd stream validation There are 2 issues with the element size handling in the command stream validation which result in too small of a size calculated when the element size is 16/32/64 bits. For NHWC format, the element size is simply missing from the calculation. The bitfield for the element size is different between IFM/IFM2 and OFM. IFM and IFM2 encode the precision in parameter bits 2:3, while OFM uses bits 1:2.	2026-08-10	7.8	CVE-2026-68316

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: fix auth_chunk_list capacity check in sctp_auth_ep_add_chunkid sctp_auth_ep_add_chunkid() uses SCTP_NUM_CHUNK_TYPES (20) as the capacity limit for ep->auth_chunk_list, allowing it to hold up to 20 chunk entries (param_hdr.length up to 24). However, the copy destination asoc->c.auth_chunks in struct sctp_cookie is only SCTP_AUTH_MAX_CHUNKS (16) entries (20 bytes). When more than 16 chunks are added, sctp_association_init() memcpy overflows the destination by up to 4 bytes. Fix by using SCTP_AUTH_MAX_CHUNKS as the capacity limit, matching the destination capacity.	2026-08-10	7.3	CVE-2026-68320
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: serialize udp bearer replicast list updates tipc_udp_rcast_add() and cleanup_bearer() both update ub->rcast.list with list_add_rcu() / list_del_rcu(), but nothing serializes them. The add runs from the encap receive softirq (via tipc_udp_rcast_disc()) without rtnl_lock(), so it can race the cleanup delete and corrupt the list: list_del corruption. prev->next should be ffff8880298d7ab8, but was ffff88802449ad38. (prev=ffff888027e3ec98) kernel BUG at lib/list_debug.c:62! RIP: __list_del_entry_valid_or_report+0x17a/0x200 Workqueue: events cleanup_bearer Call Trace: cleanup_bearer (net/tipc/udp_media.c:811) process_one_work (kernel/workqueue.c:3302) worker_thread (kernel/workqueue.c:3466) The bearer can be enabled from an unprivileged user namespace, as the TIPCv2 generic-netlink ops carry no GENL_ADMIN_PERM. Add a spinlock to struct udp_bearer and take it around the list_add_rcu() in tipc_udp_rcast_add() and the list_del_rcu() loop in cleanup_bearer() so the two writers can no longer corrupt the list. Reject a duplicate peer under the same lock before allocating, and remove tipc_udp_is_known_peer(). The old lockless pre-check in tipc_udp_rcast_disc() was racy: two softirqs discovering the same peer could both find it absent and add it twice. cleanup_bearer() runs from a workqueue after tipc_udp_disable() clears the bearer's up bit, so an encap softirq can still reach tipc_udp_rcast_add() and add a peer after cleanup_bearer() has already emptied the list, leaking that entry when the bearer is freed. Mark the bearer disabled under rcast_lock once the list is emptied and refuse further additions.	2026-08-10	7.8	CVE-2026-68323
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: airoha: Fix DMA direction for NPU mailbox buffer airoha_npu_send_msg() always maps the mailbox buffer with DMA_TO_DEVICE, but some callers expect the NPU to write response data back into the same buffer: - airoha_npu_wlan_msg_get() (NPU_OP_GET): NPU writes response into the buffer, then the caller reads it via memcpy() - airoha_npu_ppe_stats_setup() (NPU_OP_SET): NPU writes back npu_stats_addr field in the response On non-cache-coherent architectures like EN7581 (Cortex-A53 without hardware cache coherency for NPU DMA), DMA_TO_DEVICE unmap is a no-op - it does not invalidate the CPU cache. If the NPU-written cache line is still present in the CPU cache when the caller reads the buffer, the CPU observes stale data instead of the NPU response. This is a timing-sensitive bug: small mailbox buffers (~24 bytes) typically fit in a single cache line and may survive in the cache until the caller reads them, producing silent data corruption rather than a crash. The bug is more likely to trigger when the caller reads the response immediately after dma_unmap_single() without intervening cache-evicting operations. Fix by using DMA_BIDIRECTIONAL for both map and unmap, which ensures dma_unmap_single() invalidates the CPU cache on non-coherent systems. The mailbox buffers are small so there is no performance concern.	2026-08-10	7.8	CVE-2026-68330
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rds: drop incoming messages that cross network namespace boundaries rds_find_bound() looks up the destination socket using a global rhashtable keyed solely on (addr, port, scope_id). Network namespaces are not part of the key, so a sender in netns A can deliver an incoming message (inc) to a socket that lives in a different netns B. When this happens, inc->i_conn points to an rds_connection whose c_net is netns A, but the receiving rs lives in netns B. Once the child process that created netns A exits, cleanup_net() calls rds_loop_exit_net() -> rds_loop_kill_conns() -> rds_conn_destroy(), freeing that connection. If the survivor socket in netns B still holds the inc, any subsequent dereference of inc->i_conn is a use-after-free. There are two dangerous sites in rds_clear_recv_queue(): 1. inc->i_conn->c_lcong (offset 88 of freed rds_connection, size 200) read via rds_recv_rcvbuf_delta() -- confirmed by KASAN. 2. inc->i_conn->c_trans->inc_free(inc) (function pointer at offset 80) called via rds_inc_put() when the inc refcount reaches zero -- same race window,	2026-08-10	7.8	CVE-2026-68335

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	potential call-through-freed-object primitive. The bug is reachable from unprivileged user namespaces (CLONE_NEWUSER + CLONE_NEWNET), available since Linux 3.8. Fix this by rejecting the delivery in rds_rcv_incoming() when the socket returned by rds_find_bound() belongs to a different network namespace than the connection that carried the message. Use the existing rds_conn_net() / sock_net() helpers and net_eq() for the comparison.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/packet: avoid fanout hook re-registration after unregister packet_set_ring() temporarily detaches a socket from packet delivery while reconfiguring its ring. It records the previous running state, clears po->num, unregisters the protocol hook when needed, drops po->bind_lock, and later restores po->num and re-registers the hook from the saved was_running value. That unlocked window can race with NETDEV_UNREGISTER. The notifier can observe the socket as not running, skip __unregister_prot_hook(), and invalidate the per-socket binding by setting po->ifindex to -1 and clearing po->prot_hook.dev. A one-member fanout group can still retain its shared fanout hook device pointer. When packet_set_ring() resumes, re-registering solely from the stale was_running state can re-add the fanout hook after the device has been unregistered. Treat po->ifindex == -1 as an invalidated binding after reacquiring po->bind_lock. This is distinct from ifindex 0, the normal unbound/wildcard state: ifindex -1 marks an existing device binding that was invalidated when the device was unregistered. Restore po->num as before, but do not re-register the hook if device unregister already detached the socket.	2026-08-10	7.8	CVE-2026-68338
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: occ: validate poll response sensor blocks The OCC poll response parser walks a counted list of sensor data blocks. It used the static backing-array capacity as the parse boundary, but a transport response makes only data_length bytes current and valid. A truncated response can therefore make the parser consume a block header or block extent outside the current response. Use data_length as the parent boundary, prove the fixed poll header and each current block header before reading them, and prove the complete block before advancing. Keep parsed sensor metadata local until the complete response has passed validation, then publish it. Propagate malformed-response errors before publishing the OCC as active.	2026-08-10	7.7	CVE-2026-68340
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: tas2781: bound firmware description string parsing The TAS2781 firmware parser reads several variable-length description strings with strlen() before checking that the string terminator is present inside the firmware blob. A malformed firmware image without a NUL terminator can therefore make the parser walk past the end of the firmware buffer before the later size checks run. Add a small bounded string-length helper and use it for all description fields that are parsed from the firmware buffer. Keep the existing size checks for the fixed bytes that follow each string.	2026-08-10	7.1	CVE-2026-68348
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: dummy_hcd: prevent fifo_req reuse during giveback dummy_hcd embeds a single shared usb_request (dum->fifo_req) that the "emulated single-request FIFO" fast-path in dummy_queue() reuses for small IN transfers: it copies the caller's request into it (req->req = *_req) and queues it, treating list_empty(&fifo_req.queue) as "the slot is free". The completion side (dummy_timer/transfer/nuke/dummy_dequeue) follows the standard pattern: list_del_init(&req->queue) unlinks the request, then the lock is dropped and usb_gadget_giveback_request() invokes req->complete(). But list_del_init() makes fifo_req.queue look empty *before* the completion callback returns, so a concurrent dummy_queue() on another CPU sees the slot as free, reuses fifo_req and runs req->req = *_req -- overwriting req->complete while dummy_timer is mid-calling it. The indirect call then jumps to a clobbered pointer, causing a general protection fault / page fault in dummy_timer (syzkaller extid faf3a6cf579fc65591ca). The clobbering write is an in-bounds memcpy on a live shared object, so KASAN cannot flag it. Add a fifo_req_busy bit covering the shared request's whole lifetime: set it in dummy_queue() when the FIFO fast-path takes fifo_req (making it the fast-path guard, replacing the list_empty(&fifo_req.queue) test), and clear it after the completion callback has returned, via a dummy_giveback() helper used at all four gadget-request giveback sites. The shared slot can no longer be reused until its completion callback has finished.	2026-08-10	7.8	CVE-2026-68370
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: usb: core: sysfs: add lock to bos_descriptors_read() Add a lock to the function bos_descriptors_read(). This function accesses udev->bos, which could be	2026-08-10	7.8	CVE-2026-68374

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	simultaneously freed in usb_reset_and_verify_device(), a function that is commonly called in drivers all over the kernel.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_tunnel_key: Defer dst_release to RCU callback Fix a race-condition use-after-free in tunnel_key_release_params(). The function releases the metadata_dst of the old params synchronously via dst_release() while deferring the params struct free with kfree_rcu(). A concurrent tunnel_key_act() reader on the datapath may still hold the old params pointer (under rcu_read_lock_bh) and proceed to call dst_clone(&params->tcft_enc_metadata->dst) after the writer's dst_release has already pushed the dst's rcuref to RCUREF_DEAD. zdi-disclosures@trendmicro.com produced a poc which i (and Victor) verified that KASAN reports: ===== BUG: KASAN: slab-use-after-free in instrument_atomic_read_write include/linux/instrumented.h:112 BUG: KASAN: slab-use-after-free in atomic_sub_return_release include/linux/atomic/atomic-instrumented.h:326 BUG: KASAN: slab-use-after-free in __rcuref_put include/linux/rcuref.h:109 BUG: KASAN: slab-use-after-free in rcuref_put include/linux/rcuref.h:173 BUG: KASAN: slab-use-after-free in dst_release+0x5b/0x370 net/core/dst.c:168 Write of size 4 at addr ffff8806158de40 by task poc/9388 CPU: 0 UID: 0 PID: 9388 Comm: poc Tainted: G W 7.1.0-rc7 #7 PREEMPT(lazy) Tainted: [W]=WARN Hardware name: QEMU Ubuntu 25.10 PC v2 (i440FX + PIIX, + 10.1 machine, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 dump_stack_lvl+0x100/0x190 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 print_report+0x139/0x4ad mm/kasan/report.c:482 kasan_report+0xe4/0x1d0 mm/kasan/report.c:595 check_region_inline mm/kasan/generic.c:186 kasan_check_range+0x125/0x200 mm/kasan/generic.c:200 instrument_atomic_read_write include/linux/instrumented.h:112 atomic_sub_return_release include/linux/atomic/atomic-instrumented.h:326 __rcuref_put include/linux/rcuref.h:109 rcuref_put include/linux/rcuref.h:173 dst_release+0x5b/0x370 net/core/dst.c:168 refdst_drop include/net/dst.h:272 skb_dst_drop include/net/dst.h:284 skb_release_head_state+0x293/0x400 net/core/skbuff.c:1163 skb_release_all net/core/skbuff.c:1187 [...] Allocated by task 9391: kasan_save_stack+0x30/0x50 mm/kasan/common.c:57 kasan_save_track+0x14/0x30 mm/kasan/common.c:78 poison_kmalloc_redzone mm/kasan/common.c:398 __kasan_kmalloc+0x9a/0xb0 mm/kasan/common.c:415 kasan_kmalloc include/linux/kasan.h:263 __do_kmalloc_node mm/slub.c:5296 __kmalloc_noprof+0x2f1/0x830 mm/slub.c:5308 kmalloc_noprof include/linux/slab.h:954 kcalloc_noprof include/linux/slab.h:1188 offload_action_alloc+0x2f/0x130 net/core/flow_offload.c:35 tcf_action_offload_add_ex+0x1ba/0x880 net/sched/act_api.c:258 tcf_action_offload_add net/sched/act_api.c:293 tcf_action_init+0x66e/0xa20 net/sched/act_api.c:1547 tcf_action_add+0xf6/0x5d0 net/sched/act_api.c:2101 [...] Freed by task 9391: kasan_save_stack+0x30/0x50 mm/kasan/common.c:57 kasan_save_track+0x14/0x30 mm/kasan/common.c:78 kasan_save_free_info+0x3b/0x70 mm/kasan/generic.c:584 poison_slab_object mm/kasan/common.c:253 __kasan_slab_free+0x6b/0x90 mm/kasan/common.c:285 kasan_slab_free include/linux/kasan.h:235 slab_free_hook mm/slub.c:2689 slab_free mm/slub.c:6251 kfree+0x21f/0x6b0 mm/slub.c:6566 tcf_action_offload_add_ex+0x4ad/0x880 net/sched/act_api.c:284 tcf_action_offload_add net/sched/act_api.c:293 tcf_action_init+0x66e/0xa20 net/sched/act_api.c:1547 tcf_action_add+0xf6/0x5d0 net/sched/act_api.c:2101 The buggy address belongs to the object at ffff8806158de00 which belongs to the cache kcalloc-256 of size 256 The buggy address is located 64 bytes inside of freed 256-byte region [ffff8806158de00, ffff8806158df00) The buggy address belongs to the physical page: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0xffff8806158d600 pfn:0x6158c head: order:1 mapcount:0 entire_map ---truncated---	2026-08-10	7.8	CVE-2026-68377
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: fix TIME_WAIT socket reference leak on PSP policy failure Release the TIME_WAIT socket reference and jump to discard_it upon PSP policy failure in both IPv4 and IPv6 receive paths. This prevents a memory leak of tcp_tw_bucket structures.	2026-08-10	7.5	CVE-2026-68379
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix use-after-free of mm_struct in job scheduler amdxdna_cmd_submit() stores current->mm in job->mm without holding any reference. aie2_sched_job_run()	2026-08-10	7.8	CVE-2026-68380

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	later access job->mm from the DRM scheduler worker thread. With only a raw pointer and no structural reference, the mm_struct can be freed before the scheduler runs the job. Fix this by calling mmgrab() to hold a structural mm_count reference for the lifetime of the job, paired with mmdrop() in every cleanup path.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/guc: Hold device ref until queue teardown completes GuC exec queue destruction can run asynchronously. If the final device put happens from a destroy worker, drmm cleanup can end up draining the same workqueue and deadlock. Hold a drm_device reference for the queue lifetime and drop it after queue teardown completes. This keeps drmm cleanup from running while async destroy work is still pending. Move GuC destroy work to a module-lifetime Xe workqueue and flush it on PCI remove so hot-unbind/rebind still waits for pending destroy work. With queue-held device refs, guc_submit_sw_fini() cannot run with live GuC IDs. Replace the fini wait with an assertion and remove the unused fini_wq. v2: - Rebase v3: - Switch to queue-lifetime drm_dev_get()/drm_dev_put() model. (Matt) - Queue async teardown on system_dfl_wq instead of xe->destroy_wq. (Matt) - Drop separate deferred drm_dev_put worker. - Remove stale drain_workqueue(xe->destroy_wq) from guc_submit_sw_fini(). v4: - Replace the guc_submit_sw_fini() wait with an assertion and remove the now-unused fini_wq. (sashiko) v5: - Move destroy work to a module-lifetime Xe workqueue instead of system_dfl_wq. (Matt) - Flush the module-lifetime destroy workqueue during PCI remove to preserve the old device-remove wait semantics. v6: - Keep SVM pagemap destroy work on the per-device destroy_wq to avoid letting it outlive the xe_device/drm_device. (Sashiko) - Use WQ_MEM_RECLAIM for xe->destroy_wq because SVM pagemap destroy work can be queued from the reclaim path. v7: - Drop the per-device xe->destroy_wq and use the module-level destroy WQ for SVM pagemap destroy as well. (Matt) - Rename xe_exec_queue_destroy_wq_*(()) helpers to xe_destroy_wq_*(()) helpers because the WQ is no longer exec-queue specific. (Matt) v8: - Rebase. v9: - Keep SVM pagemap destroy work on the per-device WQ_MEM_RECLAIM destroy_wq because it can be queued from reclaim and embeds the dev_pagemap used by devres teardown. (Sashiko) - Keep the module-level destroy WQ GuC-only and drop WQ_MEM_RECLAIM from it. - Update the module-WQ kdoc to document the GuC/SVM split. v10: - Keep xe->destroy_wq per-cpu while adding WQ_MEM_RECLAIM to fix the workqueue allocation warning. v11: - Drop the SVM pagemap destroy comment as it was revision-specific. (Thomas) v12: - Rebase. (cherry picked from commit da1124abac689cc2b1d8995e5f0a816f8a122edb)	2026-08-10	7.8	CVE-2026-68382
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/guc: Keep scheduler timeline name alive The scheduler keeps a pointer to the timeline name, but q->name is freed with the exec queue while scheduler fences can still reference it. Store the name in struct xe_guc_exec_queue so it shares the scheduler's RCU-deferred lifetime. (cherry picked from commit 41075f0eb5dcbd3b065d15f15ef7bbe9315188e8)	2026-08-10	7.8	CVE-2026-68383
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/vf: Fix VF CCS attach/detach race with in-flight BO moves xe_bo_move() attaches VF CCS read/write batch buffers (BBs) to a BO after it transitions NULL/SYSTEM -> TT, and detaches them after it transitions TT -> SYSTEM. Both operations were done synchronously on the CPU immediately after building the move's copy/clear fence, without waiting for that fence to signal. This creates two races with VF migration: - Attach happens too late relative to the copy job it is meant to protect. If the copy job is submitted before the CCS BBs are attached, a VF migration event that pauses execution mid-copy can observe partially copied CCS metadata without the attach state needed to correctly save/restore it. - Detach happens too early relative to the copy job that moves data out of TT. The CCS BBs are torn down right after the copy fence is obtained, while the actual blit may still be in flight. A VF migration event that pauses execution mid-copy can then race the save/restore path against the still-running blit, and the CCS BBs it would need to make sense of the paused state have already been removed. Fix both races: - Move the attach call to before the copy/clear job is submitted, so the CCS BBs are already registered by the time the copy runs. On attach failure, unwind and bail out of the move. xe_migrate_ccs_rw_copy() now takes the destination resource explicitly, since bo->ttm.resource is not updated to the new resource until after the move commits. - Detach only after explicitly waiting for the copy fence to signal, instead of tearing down the CCS BBs immediately after obtaining it. While here, also fix xe_sriov_vf_ccs_attach_bo() to properly unwind and propagate errors: the per-	2026-08-10	7.8	CVE-2026-68384

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	context loop previously never broke out on error, silently discarding earlier failures. Unwind by clearing each attached context directly via xe_migrate_ccs_rw_copy_clear() instead of reusing xe_sriov_vf_ccs_detach_bo(), which requires both contexts to be attached before it will clean up either one. (cherry picked from commit d45ad0aa7a1eb5d7288b5ed948b05695611dc39e)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: raw: add locking for raw flags bitfield With commit 890e5198a6e5 ("can: raw: use bitfields to store flags in struct raw_sock") the formerly separate integer values have been integrated into a single bitfield. This led to a read-modify-write operation when changing a flag in raw_setsockopt() which now needs a locking to prevent concurrent access. Instead of adding a lock/unlock hell in each of the flag manipulations this patch introduces a wrapper for a new raw_setsockopt_locked() function analogue to the isotp_setsockopt[_locked]() approach in net/can/isotp.c [mkl: use Closes tag instead of Link]	2026-08-10	7.8	CVE-2026-68387
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: mgmt: hold reference for hci_conn in mgmt_pending_cmds Dereferencing RCU-protected pointers outside critical sections is invalid and may lead to UAF. Use of hci_conn in hci_sync callbacks also needs to hold refcount to avoid UAF. Take appropriate locks for hci_conn lookups, and take refcount for hci_conn pointers stored in mgmt_pending_cmd so that the pointer stays valid. When accessing conn->state, ensure hdev->lock is held to avoid data race.	2026-08-10	7.8	CVE-2026-68391
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: mgmt: fix locking in unpair_device/disconnect_sync Dereferencing RCU-protected pointers outside critical sections is invalid and may lead to UAF. Take hdev->lock for hci_conn lookup and hci_abort_conn(). Don't use RCU to ensure the conn is fully initialized at this point.	2026-08-10	7.8	CVE-2026-68392
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: revalidate LOAD_CONN_PARAM queued update MGMT_OP_LOAD_CONN_PARAM queues conn_update_sync() when a single parameter update changes an existing LE central connection. The queued work currently stores a borrowed hci_conn_params entry from hdev->le_conn_params. A later LOAD_CONN_PARAM request can clear disabled parameters and free that entry before hci_cmd_sync_work() runs the queued callback. Do not keep the borrowed hci_conn_params pointer in queued work. Queue the hci_conn instead and hold a reference until the queued callback completes. When the work runs, revalidate that the connection is still present, look up the current hci_conn_params entry, and cancel the update if userspace removed that entry while the work was pending. Copy the interval values from the current params entry under hdev->lock, then drop the lock and keep using hci_le_conn_update_sync() to issue the update. Validation reproduced this kernel report: BUG: KASAN: slab-use-after-free in conn_update_sync+0x2a/0xf0 [bluetooth] Read of size 1 at addr ffff88810c697126 by task kworker/u17:0/377 Workqueue: hci0 hci_cmd_sync_work [bluetooth] Call Trace: <TASK> dump_stack_lvl+0x66/0xa0 print_report+0xce/0x5f0 kasan_report+0xe0/0x110 conn_update_sync+0x2a/0xf0 [bluetooth] hci_cmd_sync_work+0x187/0x210 [bluetooth] process_one_work+0x4fd/0xbc0 worker_thread+0x2d8/0x570 kthread+0x1ad/0x1f0 ret_from_fork+0x3c9/0x540 ret_from_fork_asm+0x1a/0x30 Allocated by task 466: hci_conn_params_add+0xa6/0x240 [bluetooth] load_conn_param+0x4e1/0x850 [bluetooth] hci_sock_sendmsg+0x96b/0xf80 [bluetooth] Freed by task 474: kfree+0x313/0x590 hci_conn_params_clear_disabled+0x9b/0xc0 [bluetooth] load_conn_param+0x4bf/0x850 [bluetooth] hci_sock_sendmsg+0x96b/0xf80 [bluetooth]	2026-08-10	7.8	CVE-2026-68394
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ppp: defer channel free to an RCU grace period to fix pppol2tp RX UAF pppol2tp_rcv() runs in the L2TP UDP-encap softirq RX path: l2tp_udp_encap_rcv() -> l2tp_rcv_common() -> pppol2tp_rcv() -> ppp_input(&po->chan) It runs under rcu_read_lock() holding only an l2tp_session reference and takes NO reference on the internal PPP channel (struct channel, chan->ppp) that ppp_input() dereferences. The pppox socket is SOCK_RCU_FREE, so 'po' and the embedded ppp_channel are RCU-safe. But the internal struct channel is a separate allocation that ppp_release_channel() frees with a plain kfree(): close(data socket) -> pppol2tp_release() -> pppox_unbind_sock() -> ppp_unregister_channel() -> ppp_release_channel() -> kfree(pch) For a channel that is bound (PPPIOCGCHAN) but not attached to a ppp unit (no PPPIOCCONNECT, pch->ppp == NULL) and not bridged, teardown skips both ppp_disconnect_channel()'s synchronize_net() and	2026-08-10	7.8	CVE-2026-68398

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ppp_unbridge_channels()'s synchronize_rcu(), so the kfree() has no grace period. rcu_read_lock() in pppol2tp_recv() does not protect against a plain kfree(), so an in-flight ppp_input() on one CPU can dereference the channel just freed by close() on another CPU. The bug is reachable by an unprivileged user. Defer the channel free to an RCU callback via call_rcu() so the grace period fences any in-flight ppp_input(). The disconnect and unbridge teardown paths already fence with synchronize_net()/synchronize_rcu(); call_rcu() does the same here without stalling the close() path.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix UAF in sock clone early bailouts Similar to recent commit 9b51a6155d14 ("bpf, fork: wipe ->bpf_storage before bailouts that access it"), sk_clone() performs an initial shallow copy of the socket field ->sk_bpf_storage via sock_copy() for the cloned socket newsk. If sk_clone() bails out early (e.g. if sk_filter_charge() fails) prior to calling bpf_sk_storage_clone(), newsk->sk_bpf_storage still points to the parent socket's BPF local storage. When newsk is subsequently freed via sk_free(), the deallocation path (__sk_destruct() -> bpf_sk_storage_free()) destroys the parent socket's BPF local storage, leading to a use-after-free (UAF) on the parent socket. Fix this by resetting newsk->sk_bpf_storage to NULL immediately after sock_copy() in sk_clone(), and remove the now redundant initialization from bpf_sk_storage_clone().	2026-08-10	7.8	CVE-2026-68399
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_ffa: Fix Endpoint Memory Access Descriptor offset calculation Use the descriptor's `ep_mem_offset` to calculate the start of the endpoint memory access array and to comply with the FF-A spec instead of defaulting to `sizeof(struct ffa_mem_region)`. This requires moving `ffa_mem_region_additional_setup()` earlier in the setup flow. Also, add sanity checks to ensure the calculated descriptor offsets do not exceed `max_fragsize`.	2026-08-10	7.8	CVE-2026-68400
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_ffa: Fix out-of-bound writes in ffa_setup_and_transmit() Sashiko (locally) reports multiple out-of-bound issues in ffa_setup_and_transmit: 1) Writing ep_mem_access->reserved can write out of bounds for FFA versions < 1.2 as ffa_emad_size_get() returns 16 bytes in that case while reserved has an offset of 24. Instead of zeroing fields, memset the struct to zero first based on the FFA version. 2) Make sure there is enough size to write constituents. While at it, convert the only sizeof() in the driver that uses a type instead of variable.	2026-08-10	7.8	CVE-2026-68401
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: bound element ID read when checking non-inheritance cfg80211_is_element_inherited() reads the first data octet of the candidate element (id = elem->data[0]) to look it up in an extension non-inheritance list. It does so after testing elem->id, but without verifying that the element actually has a data octet. A zero-length extension element (WLAN_EID_EXTENSION with length 0) therefore makes it read one octet past the end of the element. _ieee802_11_parse_elems_full() runs this check for every element of a frame once a non-inheritance context exists -- e.g. while parsing a per-STA profile of a Multi-Link element in a (re)association response, or a non-transmitted BSS profile -- so a crafted frame from an AP can trigger a one-octet slab-out-of-bounds read during element parsing: BUG: KASAN: slab-out-of-bounds in cfg80211_is_element_inherited Read of size 1 ... in net/wireless/scan.c Return early (treat the element as inherited) when an extension element carries no data, mirroring the existing handling of empty ID lists. The bug was found by fuzzing ieee802_11_parse_elems_full() under KASAN.	2026-08-10	7.1	CVE-2026-68402
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: use wiphy work for socket owner autodisconnect nl80211_netlink_notify() walks the cfg80211 wireless device list when a NETLINK_GENERIC socket is released. If the socket owns a connection, the notifier queues the embedded wdev->disconnect_wk work item. That work is a plain work_struct today. NETDEV_GOING_DOWN cancels it, but a NETLINK_URELEASE notifier that already observed conn_owner_nlportid can queue it after that cancel returns. _cfg80211_unregister_wdev() then removes the wdev from the list and waits for RCU readers, but synchronize_net() does not drain work queued by such a reader. Make the autodisconnect work a wiphy_work instead. The callback already needs the wiphy mutex, and wiphy_work runs under that mutex. This lets teardown cancel pending autodisconnect work while holding the mutex, without a cancel_work_sync() vs. worker locking concern. Also cancel the wiphy work after list_del_rcu() and synchronize_net(). Any NETLINK_URELEASE notifier that had	2026-08-10	7.8	CVE-2026-68404

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	already reached the wdev list has then either queued the work and it is removed, or can no longer find the wdev.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: cancel sched scan results work on unregister cfg80211_sched_scan_results() can queue rdev->sched_scan_res_wk from a driver result notification while a scheduled scan request is present. The work callback recovers the containing cfg80211_registered_device and then locks the wiphy and walks the scheduled-scan request list. wiphy_unregister() already makes the wiphy unreachable and drains rdev work items before cfg80211_dev_free() can release the object, but it does not drain sched_scan_res_wk. A queued or running result work item can therefore cross the unregister/free boundary and access freed rdev state. The buggy scenario involves two paths, with each column showing the order within that path: scheduled-scan result path: unregister/free path: 1. cfg80211_sched_scan_results() 1. interface teardown stops and queues rdev->sched_scan_res_wk. removes the scheduled scan request. 2. cfg80211_wq starts the work 2. wiphy_unregister() drains other item and recovers rdev. rdev work items. 3. The worker locks rdev->wiphy 3. cfg80211_dev_free() destroys and and walks rdev state. frees rdev. Cancel sched_scan_res_wk in wiphy_unregister() alongside the other rdev work items. cancel_work_sync() removes a pending result notification and waits for an already running callback, so cfg80211_dev_free() cannot free rdev while this work item is still active. Validation reproduced this kernel report: BUG: KASAN: use-after-free in <pre> cfg80211_sched_scan_results_wk+0x4a6/0x530 Workqueue: cfg80211 cfg80211_sched_scan_results_wk [cfg80211] Read of size 8 Call trace: dump_stack_lvl+0x66/0xa0 print_report+0xce/0x630 cfg80211_sched_scan_results_wk+0x4a6/0x530 srso_alias_return_thunk+0x5/0xfbef5 __virt_addr_valid+0x224/0x430 kasan_report+0xac/0xe0 lockdep_hardirqs_on_prepare+0xea/0x1a0 process_one_work+0x8d0/0x18f0 (kernel/workqueue.c:3212) lock_is_held_type+0x8f/0x100 worker_thread+0x5ad/0xfdf0 __kthread_parkme+0xc6/0x200 kthread+0x31e/0x410 trace_hardirqs_on+0x1a/0x170 ret_from_fork+0x576/0x810 __switch_to+0x57e/0xe20 __switch_to_asm+0x33/0x70 ret_from_fork_asm+0x1a/0x30 </pre>	2026-08-10	7.5	CVE-2026-68414
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: clear mode callbacks after failed mode setup xfrm_state_gc_task can run long after a failed IPTFS state setup. In the reproduced case, __xfrm_init_state() cached x->mode_cbs, IPTFS setup returned -ENOMEM before publishing mode_data, and the temporary module reference from xfrm_get_mode_cbs() was dropped immediately. The dead state then kept x->mode_cbs until deferred GC ran after xfrm_ipnfts had been unloaded. Clear x->mode_cbs when mode init or clone fails before publishing mode_data. Those states never installed mode-specific state or the long-term IPTFS module pin, so deferred GC has nothing mode-specific to destroy and must not retain a callback table pointer past the temporary lookup reference. The buggy scenario involves two paths, with each column showing the order within that path: failed setup path: 1. cache x->mode_cbs 2. mode setup fails before mode_data 3. drop the temporary module ref 4. dead state keeps x->mode_cbs cached GC/unload path: 1. xfrm_state_put() queues GC work 2. xfrm_ipnfts unloads later 3. xfrm_state_gc_task runs 4. GC dereferences stale x->mode_cbs This also covers the failed clone path where clone_state() returns before publishing mode_data. Validation reproduced this kernel report: Kernel panic - not syncing: Fatal exception <pre> CONFIG_FAULT_INJECTION_STACKTRACE_FILTER=y failslab_stacktrace_filter matched xfrm_ipnfts frames ack_error=-12 FAULT_INJECTION: forcing a failure BUG: unable to handle page fault Workqueue: events xfrm_state_gc_task RIP: xfrm_state_gc_task+0x142/0x650 Modules linked in: esp4_offload xfrm_user [last unloaded: xfrm_ipnfts] Kernel panic - not syncing: Fatal exception </pre>	2026-08-10	7.8	CVE-2026-68415
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/siw: publish QP after initialization siw_create_qp() currently calls siw_qp_add() before the queues, CQ pointers, state, completion, and device list entry are ready. A QPN lookup can therefore reach a QP that is still being constructed. Move siw_qp_add() to the end of siw_create_qp(), after QP initialization and before adding the QP to the siw device list.	2026-08-10	7.8	CVE-2026-68417
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Prevent rereg_mr for non-mem regions When a QP/CQ/SRQ is created, a two step	2026-08-10	7.8	CVE-2026-68419

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	process is used where the buffer is allocated in userspace and explicitly registered with the normal reg_mr mechanism prior to creating the actual QP/CQ/SRQ object. These special registrations are indicated via an ABI field so the driver knows that they do not have a valid mkey and to skip the actual CQP command submission. Since these are real MR objects from the core's perspective, it is possible for a user application to invoke rereg_mr on them and cause a real CQP op to be emitted with the zero-initialized mkey value of 0. Fix this by preventing rereg_mr on these special regions.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: reject optional IPTFS templates in outbound policies syzbot reported a stack-out-of-bounds read in xfrm_state_find() which flows from xfrm_tmpl_resolve_one(). Commit 3d776e31c841 ("xfrm: Reject optional tunnel/BEET mode templates in outbound policies") disallowed optional tunnel and BEET in outbound policies to prevent this. Later when IPTFS added, it was not covered by that fix and can still trigger the out-of-bounds read; Extend the check to disallow optional IPTFS in outbound policies as well. IPTFS should be identical to tunnel mode. IN and FWD policies are not affected: xfrm_tmpl_resolve_one() is only reachable via the outbound path. Reproducer, before: ip link add dummy0 type dummy ip link set dummy0 up ip addr add 10.1.1.1/24 dev dummy0 ip xfrm policy add src 10.1.1.1/32 dst 10.1.1.2/32 dir out tmpl src fc00::dead:1 dst fc00::dead:2 proto esp reqid 1 mode iptfs level use tmpl src fc00::dead:1 dst fc00::dead:2 proto esp reqid 2 mode transport ping -W 1 -c 1 10.1.1.2 PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data. [64.168420] ===== [64.169977] BUG: KASAN: stack-out-of-bounds in __xfrm6_addr_hash+0x11e/0x170 [64.169977] Read of size 4 at addr ffff88800e1ffd20 by task ping/2844 [64.169977] CPU: 2 UID: 0 PID: 2844 Comm: ping Not tainted 7.1.0-rc7-00180-geb23b588430a #98 PREEMPT(full) [64.169977] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 [64.169977] Call Trace: [64.169977] <TASK> [64.169977] dump_stack_lvl+0x47/0x70 [64.169977] ? __xfrm6_addr_hash+0x11e/0x170 [64.169977] print_report+0x152/0x4b0 [64.169977] ? ksys_mmap_pgoff+0x6d/0xa0 [64.169977] ? entry_SYSCALL_64_after_hwframe+0x76/0x7e [64.169977] ? rcu_read_unlock_sched+0xa/0x20 [64.169977] ? __virt_addr_valid+0x21b/0x230 [64.169977] ? __xfrm6_addr_hash+0x11e/0x170 [64.169977] kasan_report+0xa8/0xd0 [64.169977] ? __xfrm6_addr_hash+0x11e/0x170 [64.169977] __xfrm6_addr_hash+0x11e/0x170 [64.169977] __xfrm_dst_hash+0x24/0xc0 [64.169977] xfrm_state_find+0xa2d/0x2f90 [64.169977] ? __pfx_xfrm_state_find+0x10/0x10 [64.169977] ? __pfx_ftrace_graph_ret_addr+0x10/0x10 [64.169977] ? __pfx_ftrace_graph_ret_addr+0x10/0x10 [64.169977] xfrm_tmpl_resolve_one+0x210/0x570 [64.169977] ? __pfx_xfrm_tmpl_resolve_one+0x10/0x10 [64.169977] ? __pfx_stack_trace_consume_entry+0x10/0x10 [64.169977] ? kernel_text_address+0x5b/0x80 [64.169977] ? __kernel_text_address+0xe/0x30 [64.169977] ? arch_stack_walk+0x8c/0xe0 [64.169977] ? xfrm_tmpl_resolve+0x130/0x200 [64.169977] ? __pfx_xfrm_tmpl_resolve+0x10/0x10 [64.169977] ? __pfx_xfrm_policy_inexact_lookup_rcu+0x10/0x10 [64.169977] ? __refcount_add_not_zero.constprop.0+0xb2/0x110 [64.169977] ? __pfx__refcount_add_not_zero.constprop.0+0x10/0x10 [64.169977] xfrm_resolve_and_create_bundle+0xd5/0x310 [64.169977] ? __pfx_xfrm_resolve_and_create_bundle+0x10/0x10 [64.169977] ? __pfx_xfrm_policy_lookup_bytype+0x10/0x10 [64.169977] ? __pfx_xfrm_policy_lookup_bytype+0x10/0x10 [64.169977] xfrm_lookup_with_ifid+0x3d8/0xb80 [64.169977] ? __pfx_xfrm_lookup_with_ifid+0x10/0x10 [64.169977] ? ip_route_output_key_hash+0xc6/0x110 [64.169977] ? kasan_save_track+0x10/0x30 [64.169977] xfrm_lookup_route+0x18/0xe0 [64.169977] ip4_datagram_release_cb+0x4c9/0x530 [64.169977] ? __pfx_ip4_datagram_release_cb+0x10/0x10 [64.169977] ? do_raw_spin_lock+0x71/0xc0 [64.169977] ? __pfx_do_raw_spin_lock+0x10/0x10 [64.169977] release_sock+0xb0/0x170 [64.169977] udp_connect+0x43/0x50 [64.169977] __sys_connect+0xa6/0x100 [64.169977] ? alloc_fd+0x2e9/0x300 [	2026-08-10	7.1	CVE-2026-68420

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	64.169977] ? __pfx__sys_connect+0x10/0x10 [64.169977] ? preempt_latency --- truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: IB/mad: Drop unmatched RMPP responses before reassembly Kernel-handled RMPP receive processing starts reassembly for active DATA responses before the response is matched to an outstanding send. The normal match happens later, after ib_process_rmpp_rcv_wc() has either assembled a complete message or consumed the segment. That ordering lets an unsolicited response that routes to a kernel RMPP agent by the high TID bits allocate or extend RMPP receive state before the full TID and source address are checked against a real request. A reordered burst can therefore reach the receive-side insertion path even though the response would not match any send. For kernel-handled RMPP DATA responses, require the existing ib_find_send_mad() match before entering RMPP reassembly. The matcher already checks the full TID, management class and source address/GID against the agent wait, backlog and in-flight send lists. If there is no match, drop the response without creating RMPP state. This leaves the RMPP window behavior unchanged and only rejects responses that have no corresponding request.	2026-08-10	7.1	CVE-2026-68425
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gpu: host1x: Fix use-after-free in host1x_bo_clear_cached_mappings __host1x_bo_unpin() drops the last reference to the mapping and frees it, so we can't dereference mapping afterwards. The cache itself outlives the mapping, so use the cache local variable instead.	2026-08-10	7.8	CVE-2026-68427
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: txgbe: fix heap overflow when reading module EEPROM txgbe_read_eeprom_hostif() always copies round_up(length, 4) bytes into the caller buffer, which ethtool allocates with exactly 'length' bytes. A non-4-aligned length therefore causes an out-of-bounds write. Copy only the remaining bytes on the final dword instead.	2026-08-12	7.8	CVE-2026-68440
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: don't propagate EXTENT_FLAG_LOGGING to split extent maps When btrfs_drop_extent_map_range() splits an extent map, the new split maps inherit the original map's flags through a local 'flags' variable. Commit f86f7a75e2fb ("btrfs: use the flags of an extent map to identify the compression type") changed the EXTENT_FLAG_LOGGING clearing to operate on em->flags instead of that local 'flags' copy, so a split of an extent map that is currently being logged wrongly inherits EXTENT_FLAG_LOGGING. The flag is then never cleared on the split, and when it is freed while still on the inode's modified_extents list (for example by the extent map shrinker) it trips the WARN_ON(!list_empty(&em->list)) in btrfs_free_extent_map() and leads to a use-after-free. Clear EXTENT_FLAG_LOGGING from the local 'flags' copy used for the splits and only clear EXTENT_FLAG_PINNED from em->flags, restoring the behaviour prior to f86f7a75e2fb.	2026-08-12	7.8	CVE-2026-68442
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: Prevent shader BO mappings from becoming writable vc4_gem_object_mmap() rejects a writable mapping of a validated shader BO, but leaves VM_MAYWRITE set. Userspace can map the BO read-only and then turn it writable with mprotect(). Validated shader BOs must stay read-only: the validator checks the instructions once and the GPU trusts them afterwards. A writable mapping lets userspace rewrite the code after validation, bypassing the validator. Clear VM_MAYWRITE on the read-only path so the mapping cannot be upgraded, as i915 already does for its read-only objects.	2026-08-12	7.8	CVE-2026-68445
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Validate vmw_surface_metadata::array_size This field comes from userspace and should be validated against specific limits depending on which Shader Model (SM) is available.	2026-08-12	7.8	CVE-2026-68446
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: clamp v9 CRIU control stack checkpoint copy to BO size CRIU checkpoint copies the MQD control stack using cp_hqd_cntl_stack_size from hardware without bounding it to the allocated BO region. If the HW field is larger than the queue's control stack allocation, memcpy reads past the BO into adjacent GTT memory and can leak kernel data to userspace. Store the page-aligned control stack BO size in mqd_manager and clamp checkpoint copies and reported checkpoint sizes to min(cp_hqd_cntl_stack_size, mm->ctl_stack_size). Apply the same bound for	2026-08-12	7.1	CVE-2026-68447

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	multi-XCC v9.4.3 checkpoint layout. (cherry picked from commit 6c2abd0ec09e86c6323010673766f76050e28aa3)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Validate length for CCA ECC private key requests cca_ecc2protkey() derives the copy length for the CPRB parameter block directly from the length field in the key token. Reject the request early if the token length exceeds the available space in the parameter block.	2026-08-13	7.8	CVE-2026-68451
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Validate length for CCA AES cipher key requests cca_cipher2protkey() derives the copy length for the CPRB parameter block directly from the length field in the key token. Reject the request early if the token length exceeds the available space in the parameter block.	2026-08-13	7.8	CVE-2026-68452
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Fix buffer over-read in cca_cipher2protkey Add validation of both the actual key buffer size and token length fields in all the cca_check_sec*token() functions. Additionally check in cca_gencipherkey() for possible underflow with returned key size. The CCA token structures contain user-controlled len fields that were used in operations without proper validation against both the actual buffer size and minimum token structure size. An attacker could set this field larger than the actual buffer size, leading to reading beyond buffer boundaries. This may result in a kernel crash or exposure of memory via sending this as part of a request down to the crypto card. Also an attacker could have used a very small len value and thus enforce a buffer under-run which may produce similar effects as a over-read. So now a key must - key buf length must be at least sizeof the token struct - the key len field inside the token must fit into the range of sizeof key token struct ... key buf length	2026-08-13	7.1	CVE-2026-68453
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: binder: cache secctx size before release zeroes it binder_transaction() bounds the scatter-gather buffer area with sg_buf_end_offset and subtracts the aligned LSM context size because the secctx is written at the tail of that area. The subtraction reads lsmctx.len, but that field has already been cleared by the time the line runs: security_secid_to_secctx(secid, &lsmctx) /* lsmctx.len set */ lsmctx_aligned_size = ALIGN(lsmctx.len, sizeof(u64)) extra_buffers_size += lsmctx_aligned_size ... security_release_secctx(&lsmctx) /* memset zeroes len */ ... sg_buf_end_offset = sg_buf_offset + extra_buffers_size - ALIGN(lsmctx.len, sizeof(u64)) /* ALIGN(0,8) */ security_release_secctx() does memset(cp, 0, sizeof(*cp)), so lsmctx.len reads back as 0 and the subtraction contributes nothing, leaving sg_buf_end_offset too large by the aligned secctx size on every transaction to a txn_security_ctx node. Each BINDER_TYPE_PTR object then derives buf_left = sg_buf_end_offset - sg_buf_offset as the sole upper bound on its copy, so the inflated end offset lets the copy run into the bytes that already hold the secctx. The aligned size must therefore be cached before release rather than re-read from the now-cleared field. Fix by caching it in lsmctx_aligned_size at function scope when it is first computed and subtracting lsmctx_aligned_size instead of re-reading lsmctx.len after release. Reuse the same value for the earlier buf_offset computation.	2026-08-15	7.8	CVE-2026-68458
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: device property: initialize the remaining fields of fwnode_handle in fwnode_init() If a firmware node is allocated on the stack (for instance: temporary software node whose life-time we control) or on the heap - but using a non-zeroing allocation function - and initialized using fwnode_init(), its secondary pointer will contain uninitialized memory which likely will be neither NULL nor IS_ERR() and so may end up being dereferenced (for example: in dev_to_swnode()). Set fwnode->secondary to NULL on initialization. While at it: initialize the remaining fields of struct fwnode_handle too just to be sure. [Fix typo in commit message. - Danilo]	2026-08-15	7.8	CVE-2026-68461
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject negative const offsets for buffer pointers The verifier rejects variable offsets for PTR_TO_TP_BUFFER and PTR_TO_BUF accesses, but it currently accepts a constant negative offset produced by pointer arithmetic. Commit 022ac0750883 ("bpf: use reg->var_off instead of reg->off for pointers") moved constant pointer offsets from reg->off to reg->var_off. However, __check_buffer_access() continued to check only the instruction offset. An access with reg->var_off equal to -8 and an instruction offset of zero therefore passes verification. For writable raw tracepoints, the access end is also calculated from the unsigned reg->var_off.value. An eight-byte access starting at -8 wraps the calculated end to zero, allowing the program to load and attach without increasing max_tp_access. After ensuring that	2026-08-15	7.8	CVE-2026-68462

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	reg->var_off is constant, calculate the effective access start using signed arithmetic and reject it when it is negative. Use the validated start to calculate the access end for both PTR_TO_TP_BUFFER and PTR_TO_BUF.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mtd: mchp23k256: use SPI match data for chip caps The driver stores chip capacity information in both the OF match table and the SPI id table. Probe currently uses of_device_get_match_data(), so a non-OF SPI modalias match falls back to mchp23k256_caps even when the SPI id table selected a different part. Use spi_get_device_match_data() so SPI id-table driver_data is consumed when OF match data is absent. This keeps the existing default fallback while avoiding the wrong MTD geometry for id-table-only matches.	2026-08-15	7.8	CVE-2026-68467
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: powerpc/uaccess: correct check for CONFIG_PPC_E500 in mask_user_address() mask_user_address() incorrectly checks for CONFIG_E500 instead of CONFIG_PPC_E500, causing mask_user_address_isel() to not be used on E500 hardware. Fix the check to use the correct name.	2026-08-15	7.8	CVE-2026-68473
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: powerpc/spufs: fix out-of-bounds access in spufs_mem_mmap_access() spufs_mem_mmap_access() computes the local store offset as address - vma->vm_start, but bounds-checks it against vma->vm_end instead of the local store size. On 64-bit, offset is always well below vma->vm_end, so the clamp never fires and len stays unbounded against the LS_SIZE buffer returned by ctx->ops->get_ls(). Reject offsets at or beyond LS_SIZE and clamp len to the remaining space, mirroring the guard already used by spufs_mem_mmap_fault() and spufs_ps_fault().	2026-08-15	7.8	CVE-2026-68474
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btrtl: validate firmware patch bounds rtlbt_parse_firmware() copies patch_length - 4 bytes before appending the firmware version. A malformed firmware patch shorter than the version field can make this subtraction underflow and turn the copy into an oversized read and write during Bluetooth setup. The existing patch_offset + patch_length check can also wrap on 32-bit architectures. Validate the patch length and range without arithmetic overflow before allocating or copying the patch.	2026-08-15	7.8	CVE-2026-68479
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rt2x00: avoid full teardown before work setup in probe rt2x00lib_probe_dev() uses the full rt2x00lib_remove_dev() teardown for all probe failures. However, drv_data allocation and workqueue allocation can fail before intf_work, autowakeup_work and sleep_work have been initialized. Do not enter the full remove path until the probe has reached the point where those work items are set up. Return directly for drv_data allocation failure, and use a small early cleanup path for workqueue allocation failure. This issue was found by our static analysis tool and then confirmed by manual review of rt2x00lib_probe_dev() and rt2x00lib_remove_dev(). The early probe exits should not call a common teardown path that assumes the later work setup has already completed. A QEMU PoC forced alloc_ordered_workqueue() to fail before the work initializers are reached. The resulting fail path entered rt2x00lib_remove_dev(), and DEBUG_OBJECTS reported invalid work drains with rt2x00lib_probe_dev() and rt2x00lib_remove_dev() in the stack.	2026-08-15	7.8	CVE-2026-72005
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: pmdomain: imx93-blk-ctrl: Extract PHY as shared domain for DSI/CSI The MIPI DSI and CSI domains share control bits for clock and reset, which can lead to incorrect behavior if one domain disables the shared resource while the other is still active. To fix the issue, introduce a shared MIPI PHY power domain to own the common resources and make DSI and CSI its subdomains. This ensures the shared bits are properly managed and not disabled while still in use.	2026-08-15	7.8	CVE-2026-72009
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tracing/osnoise: Call synchronize_rcu() when unregistering This ensures that any RCU readers traversing the instance list have finished, before releasing the reference on the tracer that the instance points to.	2026-08-15	7.8	CVE-2026-72012
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dlibs: loopback: validate offset and size in move_data() The loopback move_data() performs a memcpy into the registered DMB without checking whether offset + size exceeds the DMB length. Unlike real ISM hardware, which enforces memory region bounds natively, the software loopback has no such protection. A peer-supplied out-of-	2026-08-15	7.8	CVE-2026-72018

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bounds offset or oversized write would result in an OOB write past the allocated kernel buffer. Add an explicit bounds check before the memcpy to reject such requests with -EINVAL.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: macsec: don't read an unset MAC header in macsec_encrypt() macsec_encrypt() reads the Ethernet header via eth_hdr(skb) (skb->head + skb->mac_header) to memmove() the 12 source/destination MAC bytes forward and make room for the SecTAG. On the AF_PACKET SOCK_RAW + PACKET_QDISC_BYPASS transmit path the skb reaches the macsec ndo_start_xmit() with the MAC header unset, so eth_hdr(skb) resolves to skb->head + (u16)~0 and the read is out of bounds: a 12-byte heap over-read that is also emitted on the wire as the frame's outer source/destination MAC. KASAN reports a slab-out-of-bounds read in macsec_start_xmit() on 6.0; on current mainline a CONFIG_DEBUG_NET build flags it as an unset mac header in skb_mac_header(). On the TX path the L2 header is at skb->data, so use skb_eth_hdr(), added by commit 96cc4b69581d ("macvlan: do not assume mac_header is set in macvlan_broadcast()") for exactly this purpose.	2026-08-15	7.3	CVE-2026-72019
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mac802154: remove interfaces with RCU list deletion Queue wake, stop, and disable paths walk local->interfaces under RCU. The bulk hardware teardown path removes entries with list_del(), so an asynchronous transmit completion can follow a poisoned list node in ieee802154_wake_queue(). Use list_del_rcu() as in the single-interface removal path. The following unregister_netdevice() waits for in-flight RCU readers before freeing the netdevice, so no separate grace-period wait is needed.	2026-08-15	7.8	CVE-2026-72024
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/compaction: handle free_pages_prepare() properly in compaction_free() free_pages_prepare() can fail but compaction_free() does not handle the failure case. Failed pages should not be added back to cc->freepages for future use, since they can be either PageHWPoison or free_page_is_bad() and might cause data corruption.	2026-08-15	7.8	CVE-2026-72027
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fhandle: reject detached mounts in capable_wrt_mount() The recent fhandle RCU fix moved the mount namespace capability check into capable_wrt_mount(), so a non-NULL mnt_namespace survives the ns_capable() dereference. The helper still assumes the later READ_ONCE(mount->mnt_ns) must be non-NULL because may_decode_fh() checked is_mounted() first. That assumption is not stable. A detached mount from open_tree(..., OPEN_TREE_CLONE) can be dissolved on fput while open_by_handle_at() is between those checks, and umount_tree() can clear mount->mnt_ns. If the helper observes NULL, it dereferences mnt_ns->user_ns and panics. Return false when the RCU read observes a detached mount. This keeps the relaxed permission path conservative: a mount no longer attached to a namespace cannot authorize open_by_handle_at() access.	2026-08-15	7.8	CVE-2026-72034
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_multiq: Replace direct dequeue call with peek and qdisc_dequeue_peeked multiq_dequeue() takes a packet from a band's child with a direct ->dequeue() call after multiq_peek() peeked it. When the child is non-work-conserving the peek stashes the skb in the child's gso_skb, so the direct dequeue returns a different skb and orphans the stash, desyncing the child's qlen/backlog. With a qfq child reached through a peeking parent (e.g. tbf) this re-enters the child on an emptied list and dereferences NULL, panicking the kernel from softirq on ordinary egress. Take the packet through qdisc_dequeue_peeked(), as sch_prio already does and as sch_red and sch_sfb were just fixed to do. The helper is a no-op when the child has no stash, so a work-conserving child is unaffected.	2026-08-15	7.8	CVE-2026-72036
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipmi: Fix user refcount underflow in event delivery ipmi_alloc_recv_msg(user) takes the temporary user reference owned by the receive message, and ipmi_free_recv_msg() drops it again. If event delivery fails after allocating receive messages for earlier users, handle_read_event_rsp() rolls those messages back with ipmi_free_recv_msg(). That rollback path still drops user->refcount explicitly after freeing each message. The extra put can free a user that remains linked on intf->users, so later event delivery may dereference a freed user or trip refcount_t's addition-on-zero warning when ipmi_alloc_recv_msg() tries to acquire another reference. Remove the stale explicit put and the now-dead user assignment. Keep the list_del() and ipmi_free_recv_msg() calls; they are the required rollback operations.	2026-08-15	7.8	CVE-2026-72042

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Fix missing dirty page tracking in {pte,pmd}_wrprotect() When hardware page table walker (PTW) is enabled on LoongArch, the CPU may set _PAGE_DIRTY directly in the page table entry during a write TLB miss, without going through the software TLB store handler. The software TLB store handler (tlbex.S:254) sets both _PAGE_DIRTY and _PAGE_MODIFIED together: ori t0, t0, (_PAGE_VALID _PAGE_DIRTY _PAGE_MODIFIED) Since hardware PTW only sets _PAGE_DIRTY, the software-only bit, i.e. _PAGE_MODIFIED is left unchanged. This creates a window where a PTE has _PAGE_DIRTY set (hardware knows the page is dirty) but _PAGE_MODIFIED clear (software is unaware). When fork()/clone() triggers copy-on-write, __copy_present_ptes() calls pte_wrprotect(), which unconditionally clears both the _PAGE_WRITE and _PAGE_DIRTY bits: pte_val(pte) &= ~(_PAGE_WRITE _PAGE_DIRTY); Since _PAGE_MODIFIED was never set, the dirtiness information is lost completely. Subsequently, when memory pressure triggers page reclaim, page_mkclean() / try_to_unmap() sees the page as clean (i.e. pte_dirty() returns false) and the page may be freed without writeback, causing data corruption. Fix this by propagating the _PAGE_DIRTY bit to the _PAGE_MODIFIED bit in both pte_wrprotect() and pmd_wrprotect() before clearing writeable bits: if (pte_val(pte) & _PAGE_DIRTY) pte_val(pte) = _PAGE_MODIFIED; The pmd_wrprotect() fix handles the CONFIG_TRANSPARENT_HUGEPAGE case, where pmd entries need the same treatment. This ensures the software dirty tracking bit (checked by pte_dirty() and pmd_dirty()), which read both the _PAGE_DIRTY and _PAGE_MODIFIED bits) is preserved across fork COW write-protection. The issue was found by the LTP madvise09 test case, which exercises page reclaim after "madvise(MADV_FREE), write and fork" operation sequence on private anonymous mappings.	2026-08-15	7.1	CVE-2026-72043
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ieee802154: admin-gate legacy LLSEC dump operations In net/ieee802154/netlink.c, the legacy IEEE802154_NL family ops table builds the LLSEC dump entries (LLSEC_LIST_KEY, LLSEC_LIST_DEV, LLSEC_LIST_DEVKEY, LLSEC_LIST_SECLEVEL) with IEEE802154_DUMP() which sets no .flags, so generic netlink runs them ungated. The modern nl802154 family admin-gates the equivalent reads via NL802154_CMD_GET_SEC_KEY and friends with .flags = GENL_ADMIN_PERM. Any local uid that can open AF_NETLINK / NETLINK_GENERIC can resolve the "802.15.4 MAC" family and dump LLSEC_LIST_KEY on any wpan netdev that has an LLSEC key installed; the dump handler writes the raw 16-byte AES-128 key bytes (IEEE802154_ATTR_LLSEC_KEY_BYTES, copied verbatim from struct ieee802154_llsec_key.key) into the reply. Recovering the AES key compromises 802.15.4 LLSEC link confidentiality and authenticity, since LLSEC uses CCM* and the same key authenticates and encrypts frames. Impact: any local uid with no capabilities can read the raw 16-byte AES-128 LLSEC key from the kernel keytable on any wpan netdev that has an administrator-installed LLSEC key, by issuing an LLSEC_LIST_KEY dump on the legacy IEEE802154_NL generic-netlink family. Introduce IEEE802154_DUMP_PRIV() mirroring IEEE802154_DUMP() but setting .flags = GENL_ADMIN_PERM, and use it for the four LLSEC dump entries. LIST_PHY and LIST_IFACE retain IEEE802154_DUMP() because the modern nl802154 family exposes their equivalents to unprivileged readers by design (NL802154_CMD_GET_WPAN_PHY and NL802154_CMD_GET_INTERFACE carry "can be retrieved by unprivileged users" annotations).	2026-08-15	7.1	CVE-2026-72049
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: cpu: hotplug: Bound hotplug states sysfs output states_show() adds CPU hotplug state names into a single sysfs buffer using sprintf(). With enough registered states, this can write past the end of the PAGE_SIZE buffer. Use sysfs_emit_at() so output is bounded.	2026-08-15	7.8	CVE-2026-72066
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: cpu: hotplug: Preserve per instance callback errors cpuhp_invoke_callback() unwinds earlier callbacks for the same hotplug state when one instance fails. The rollback path currently reuses ret, so a successful rollback can hide the original error and make the failed transition look successful. Keep the rollback result separate from the original error.	2026-08-15	7.8	CVE-2026-72067
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tracing/user_events: Fix use-after-free in user_event_mm_dup() user_event_mm_dup() walks the parent mm's enabler list locklessly under rcu_read_lock() during fork() (from copy_process()); it does not take event_mutex: rcu_read_lock(); list_for_each_entry_rcu(enabler, &old_mm->enablers,	2026-08-15	7.8	CVE-2026-72071

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mm_enablers_link) enabler->event = user_event_get(orig->event); user_event_enabler_destroy() removes an enabler from that list with list_del_rcu() and then, without waiting for a grace period, drops the enabler's user_event reference with user_event_put() and frees the enabler with kfree(). A reader that loaded the enabler before the list_del_rcu() can still be walking it, which leads to two use-after-frees: - kfree(enabler) frees the enabler while that reader dereferences enabler->event. - user_event_put() may drop the last reference to the user_event, which is then freed (via delayed_destroy_user_event() on a work queue), while the same reader does user_event_get(orig->event) on it. Both are reachable by an unprivileged task that can open user_events_data: one multithreaded process that registers an enabler and then concurrently unregisters it and calls fork() triggers the race. KASAN reports a slab-use-after-free in user_event_mm_dup() during clone(), with a "refcount_t: addition on 0" warning when the user_event is freed. The enabler use-after-free was found first; the user_event one was reported by XIAO WU, and the earlier enabler-only fix did not address it. Defer both the user_event_put() and the kfree(enabler) to a work item queued with queue_rcu_work(), so they run only after an RCU grace period, once all readers walking the enabler list have finished. The put must run in process context because user_event_put() takes event_mutex on the last reference, so a work queue is used rather than call_rcu(). The now-unlocked put lets the locked argument of user_event_enabler_destroy() be removed; all callers are updated.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: macsec: fix use-after-free of metadata_dst on RX SC delete When an offloaded MACsec RX SC is deleted, macsec_del_rxsc_ctx() freed the per-SC metadata_dst with metadata_dst_free(), which kfree()s the object unconditionally and ignores the dst reference count. The RX datapath in mlx5e_macsec_offload_handle_rx_skb() looks up the SC under rcu_read_lock() via xa_load(), takes a reference with dst_hold() and attaches the dst to the skb with skb_dst_set(). A reader that already obtained the rx_sc pointer can race with the delete path and operate on freed memory. Fix the owner side by dropping the reference with dst_release() instead of freeing unconditionally, and convert the RX datapath to dst_hold_safe() so a reader racing the SC delete cannot attach a dst whose last reference was just dropped; only attach it when a reference was actually taken. mlx5e_macsec_add_rxsc() also published sc_xarray_element via xa_alloc() before rx_sc->md_dst was allocated and initialised, so a datapath reader that looked the SC up by fs_id could observe rx_sc with md_dst still NULL or, on weakly-ordered architectures, a non-NULL md_dst pointer whose contents were not yet visible. NULL-check the xa_load() result and md_dst on the datapath, and reorder add_rxsc() so the xa_alloc() publish happens only after md_dst is fully initialised; the xarray RCU publish then pairs with the rcu_read_lock()/xa_load() in the datapath. Note: macsec_del_rxsc_ctx() also kfree()s rx_sc->sc_xarray_element without an RCU grace period while the same datapath reads it under rcu_read_lock(); that is a separate pre-existing issue left to a follow-up patch. Found by Osec automated security-research tooling (https://0sec.ai).	2026-08-15	7.8	CVE-2026-72072
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/resctrl: Fix use-after-free during unmount During unmount or failure teardown all mon_data structures that contain monitoring event file private data are freed after which kernfs nodes are removed. However, the RDT_DELETED flag is never set for the statically allocated default resource group. A concurrent reader of an event file associated with the default resource group may, after dropping kernfs active protection, block on rdtgroup_mutex while unmount proceeds to free the file private data and destroy the kernfs node without waiting for the reader. When the mutex is released, the reader wakes up, observes that RDT_DELETED is not set for the default group, and dereferences the already-freed file private data. The scenario can be depicted as follows: CPU0 CPU1 /* * Default resource group's * monitoring data accessible via * kernfs file with kernfs_node::priv * pointing to a struct mon_data. * User opens the file for reading. */ rdtgroup_mondata_show() /* arch encounters fatal error */ rdtgroup_kn_lock_live() resctrl_exit() atomic_inc(&rdtgroup_default.waitcount) cpus_read_lock() kernfs_break_active_protection(kn) mutex_lock(&rdtgroup_mutex) cpus_read_lock() resctrl_fs_teardown() mutex_lock(&rdtgroup_mutex) rmdir_all_sub() mon_put_kn_priv() /* Delete all mon_data structures */ rdtgroup_destroy_root() kernfs_destroy_root() rdtgroup_default.kn = NULL mutex_unlock(&rdtgroup_mutex) /* * rdtgroup_default.flags is empty so * rdtgroup_kn_lock_live() returns * &rdtgroup_default */ md = of->kn->priv; /* md	2026-08-15	7.8	CVE-2026-72080

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	points to freed mon_data */ Set RDT_DELETED for the default group unconditionally since the flag does not lead to the freeing of this statically allocated group. Do not allow a new resctrl mount if there are any waiters on default group of previous mount. A new mount will re-initialize the default group that would appear to waiters from previous mount as though the default group is accessible causing them to access the mon_data structures from the previous mount that have been removed.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Reject firmware log with size smaller than header fw_log_from_bo() validates the tracing buffer header_size and that the log fits within the BO, but never checks that log->size is at least log->header_size. fw_log_print_buffer() then computes: u32 data_size = log->size - log->header_size; which underflows to a near-U32_MAX value when firmware reports a log whose size is smaller than its header. That huge data_size defeats the log_start/log_end bounds clamps added by commit dd1311bcf0e6 ("accel/ivpu: Add bounds checks for firmware log indices"), so fw_log_print_lines() reads far past the small real data region of the BO. A size of 0 also makes fw_log_from_bo() advance the offset by 0, causing the callers to loop forever on the same header. Reject logs whose size is smaller than the header (which also rejects size == 0).	2026-08-15	7.1	CVE-2026-72089
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Use caller client for debug BO sync amdxdna_drm_sync_bo_ioctl() looks up args->handle in the ioctl caller's drm_file. For SYNC_DIRECT_FROM_DEVICE, it then calls amdxdna_hwctx_sync_debug_bo(), but passes abo->client. amdxdna_hwctx_sync_debug_bo() uses the passed client both as the handle namespace for debug_bo_hdl and as the owner of the hardware context xarray. Those must match the file that supplied args->handle. The BO's stored client pointer is object state, not the ioctl context. Pass filp->driver_priv instead, matching the original handle lookup.	2026-08-15	7.8	CVE-2026-72090
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix use-after-free in amdxdna_gem_dmabuf_mmap() When vm_insert_pages() fails, the error path calls vma->vm_ops->close(vma) which internally calls drm_gem_vm_close() â†’ drm_gem_object_put(), releasing the GEM object reference acquired at the start of the function. However, the close_vma label then falls through to put_obj, which calls drm_gem_object_put() a second time on the same object. If the first put releases the last reference, the object is freed and the second put accesses freed memory, causing a use-after-free. Fix by returning directly from close_vma instead of falling through to put_obj, since the close handler already performs all necessary cleanup including the object put.	2026-08-15	7.8	CVE-2026-72093
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dma-fence: Make dma_fence_dedup_array() robust against 0-count input dma_fence_dedup_array() returns 1 when called with num_fences == 0: the for-loop body never executes, j stays at 0, and the final 'return ++j' yields 1. This contradicts both the kernel-doc ("Return: Number of unique fences remaining in the array") and the natural expectation that 0 input gives 0 output. The caller __dma_fence_unwrap_merge() bails out via the 'if (count == 0 count == 1)' fast path and so is safe. But amdgpu_userq_wait_*() could reach the dedup call with a zero local count and dereference an uninitialized fence slot in the array. Make the contract match the documentation by returning 0 early. This also skips an unnecessary sort() call on an empty array.	2026-08-15	7.8	CVE-2026-72095
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm-integrity: don't increment hash_offset twice hash_offset is already incremented in the loop "for (i = 0; i < to_copy; i++, ts--)". Do not increment it again.	2026-08-15	7.1	CVE-2026-72099
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm_early_create: fix freeing used table on dm_resume failure If dm_resume fails, the kernel attempts to free table with dm_table_destroy, but the table was already instantiated with dm_swap_table. This commit skips the call to dm_table_destroy in this case.	2026-08-15	7.8	CVE-2026-72102
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm: avoid leaking the caller's thread keyring via the table device file The refactoring in commit a28d893eb327 ("md: port block device access to file") accidentally causes the caller's thread keyring to be kept alive long beyond the caller's lifetime. As a result, "cryptsetup luksSuspend" silently fails to wipe the LUKS volume key from memory. In detail: "cryptsetup luksOpen" uses its supposedly ephemeral thread keyring to pass the volume key to the kernel. dm-crypt's crypt_set_keyring_key() copies the	2026-08-15	7.3	CVE-2026-72103

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	key material into its own crypt_config structure and then drops its own reference to the key in the keyring with key_put(). With this fix, restoring pre-v6.9 behavior, the copy in the thread keyring is then promptly garbage collected, such that exactly one copy of the volume key remains. This single copy is correctly wiped from memory on "cryptsetup luksSuspend". Without this fix, the thread keyring and the volume key in it remains. This second copy is only freed on "luksClose". "luksSuspend" neither knows about this copy nor has any way to remove it, so the key remains recoverable from RAM after a suspend that is documented to have wiped it. This fix should not introduce new security problems, as the code is anyway gated by CAP_SYS_ADMIN. The device-mapper core, not the calling task, is the legitimate owner of this long-lived file.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm-log: fix a bitset_size overflow on 32bit machines Commit c20e36b7631d ("dm log: fix out-of-bounds write due to region_count overflow") made sure that region_count could fit in an unsigned int. But the bitmap memory isn't allocated based on region_count. It uses bitset_size (a size_t variable). The first step of calculating bitset_size is to set it to region_count, rounded up to a multiple of BITS_PER_LONG. If region_size is less than BITS_PER_LONG smaller than UINT_MAX, it will get rounded up to 2^32. On a 32bit architecture, this will make bitset_size wrap around to 0 and fail, despite region_count being valid. Since bitset_size gets divided by 8, it can hold any valid region_count. It just needs a special case to handle the rollover. If it is 0, the value rolled over, and bitset size should be set to the number of bytes needed to hold 2^32 bits.	2026-08-15	7.8	CVE-2026-72105
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm thin metadata: fix metadata snapshot consistency on commit failure __reserve_metadata_snap() and __release_metadata_snap() modify the superblock's held_root directly in the block_manager's buffer. If the subsequent metadata commit fails, the held_root gets flushed to disk through the abort_transaction path, resulting in inconsistent metadata. Reproducer 1: __reserve_metadata_snap() 1. Create a 2 MiB metadata device and make the region after the 14th block inaccessible, to trigger metadata commit failure in the subsequent reserve_metadata_snap operation. The 14th block will be the shadow destination for the index block. dmsetup create tmeta --table "0 112 linear /dev/sdc 0 112 3984 error" 2. Create a 16 MiB thin-pool dmsetup create tdata --table "0 32768 zero" dd if=/dev/zero of=/dev/mapper/tmeta bs=4k count=1 dmsetup create tpool --table "0 32768 thin-pool /dev/mapper/tmeta \ /dev/mapper/tdata 128 0 1 skip_block_zeroing" 3. Take a metadata snapshot to trigger metadata commit failure and transaction abort. However, the held_root is written to disk, breaking metadata consistency. dmsetup message tpool 0 "reserve_metadata_snap" thin_check v1.2.2 result: Bad reference count for metadata block 6. Expected 2, but space map contains 1. Bad reference count for metadata block 7. Expected 2, but space map contains 1. Bad reference count for metadata block 13. Expected 1, but space map contains 0. Reproducer 2: __release_metadata_snap() 1. Create a 2 MiB metadata device and make the region after the 16th block inaccessible, to trigger metadata commit failure in the subsequent release_metadata_snap operation. The 16th block will be the shadow destination for the index block. dmsetup create tmeta --table "0 128 linear /dev/sdc 0 128 3968 error" 2. Create a 16 MiB thin-pool dmsetup create tdata --table "0 32768 zero" dd if=/dev/zero of=/dev/mapper/tmeta bs=4k count=1 dmsetup create tpool --table "0 32768 thin-pool /dev/mapper/tmeta \ /dev/mapper/tdata 128 0 1 skip_block_zeroing" 3. Reserve then release the metadata snapshot, to trigger metadata commit failure and transaction abort. The held_root gets removed from the on-disk superblock, causing inconsistent metadata. dmsetup message tpool 0 "reserve_metadata_snap" dmsetup message tpool 0 "release_metadata_snap" thin_check v1.2.2 result: Bad reference count for metadata block 6. Expected 1, but space map contains 2. Bad reference count for metadata block 7. Expected 1, but space map contains 2. 1 metadata blocks have leaked. Fix by deferring the held_root update to commit time. Additionally, move the existing-snapshot check in __reserve_metadata_snap before the shadow operation to avoid unnecessary work. In __release_metadata_snap, clear pmd->held_root before btree deletion so partial failure leaks blocks rather than leaving a stale reference, and unlock the snapshot block before decrementing its refcount.	2026-08-15	7.8	CVE-2026-72108
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: sparx5: unregister blocking notifier on init failure sparx5_register_notifier_blocks() registers the switchdev blocking notifier before allocating the ordered workqueue.	2026-08-15	7.8	CVE-2026-72109

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	If the workqueue allocation fails, the error path unregisters the switchdev and netdevice notifiers, but leaves the blocking notifier registered. Add a separate error label for the workqueue allocation failure path and unregister the switchdev blocking notifier there.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf, fork: wipe ->bpf_storage before bailouts that access it Currently, copy_process() can bail out to free_task() before p->bpf_storage has been initialized, with this call graph (shown here for the ICONFIG_MEMCG case): copy_process dup_task_struct arch_dup_task_struct [copies the entire task_struct, including ->bpf_storage member] [RLIMIT_NPROC check fails] delayed_free_task free_task bpf_task_storage_free rcu_dereference(task->bpf_storage) bpf_local_storage_destroy In this case, the nascent task's ->bpf_storage member that bpf_local_storage_destroy() operates on is a plain copy of the parent's ->bpf_storage pointer, not a real initialized pointer. This leads to badness (kernel hangs, UAF). This is reachable as long as the process calling fork() has been inserted into a task storage map.	2026-08-15	7.8	CVE-2026-72110
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: io_uring/bpf-ops: reject re-registration of an already-bound ops io_install_bpf() only rejects a second registration on the ctx side (ctx->bpf_ops) and sets the per-map back-pointer ops->priv unconditionally. The struct_ops link path never advances a map past BPF_STRUCT_OPS_STATE_READY, so the same io_uring_bpf_ops map can be registered more than once, and bpf_io_reg() re-resolves the target ring via fget(ops->ring_fd) on every call. A caller can therefore point the same ring_fd at a different io_ring_ctx between two BPF_LINK_CREATE calls. The second registration passes the ctx->bpf_ops check (the new ctx has none) and overwrites ops->priv, orphaning the first ctx. Teardown (io_eject_bpf()/bpf_io_unreg()) only reaches a ctx through ops->priv, so the orphaned ctx is never torn down: its ctx->loop_step keeps pointing into the struct_ops trampoline, which is freed once the map is gone. A later io_uring_enter() on the orphaned ring then calls the dangling ctx->loop_step from io_run_loop() -- a use-after-free of freed executable memory, reachable by a task with CAP_BPF + CAP_PERFMON. Reject registration when ops->priv is already set, as hid_bpf_reg() does for its struct_ops.	2026-08-15	7.8	CVE-2026-72112
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: add missing device refcount for CAN filter removal sashiko-bot remarked a problem with a concurrent device unregistration in isotp.c which also is present in the bcm.c code. A former fix for raw.c commit c275a176e4b6 ("can: raw: add missing refcount for memory leak fix") introduced a netdevice_tracker which solves the issue for bcm.c too. bcm_release(), bcm_delete_rx_op() and bcm_notifier() relied on dev_get_by_index(ifindex) to re-find the device for an rx_op before unregistering its filter. If a concurrent NETDEV_UNREGISTER has already unlisted the device from the ifindex table, that lookup fails and can_rx_unregister() is silently skipped, leaving a stale CAN filter pointing at the soon-to-be-freed bcm_op/socket. Hold a netdev_hold()/netdev_put() tracked reference on op->rx_reg_dev from the moment the rx filter is registered in bcm_rx_setup() until it is unregistered in bcm_rx_unreg(), and use that reference directly in bcm_release() and bcm_delete_rx_op() instead of re-looking the device up by ifindex.	2026-08-15	7.8	CVE-2026-72113
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: validate frame length in bcm_rx_setup() for RTR replies bcm_tx_setup() validates cf->len against the CAN/CAN FD DLC limits before installing frames for TX_SETUP, but bcm_rx_setup() never did the same for the RTR-reply frame configured via RX_SETUP with RX_RTR_FRAME.	2026-08-15	7.8	CVE-2026-72114
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: fix stale rx/tx ops after device removal RX: an RX_SETUP update(!) for an existing op skipped can_rx_register() unconditionally, even when a concurrent NETDEV_UNREGISTER had already torn down its registration (op->rx_reg_dev == NULL). This silently did not re-enable frame delivery for that updated filter. bcm_rx_setup() now re-registers in that case, while leaving rx_ops with ifindex = 0 (all CAN devices) which never carry a tracked rx_reg_dev registered as-is. TX: bcm_notify() only handled bo->rx_ops on NETDEV_UNREGISTER, leaving tx_ops with an active cyclic transmission re-arming its hrtimer indefinitely to execute bcm_tx_timeout_handler(). Cancelling the hrtimer prevents the runaway timer and any injection into a later reused ifindex, since nothing else calls bcm_can_tx() for the op until an explicit TX_SETUP update re-arms it. Unlike bcm_rx_unreg(), which clears the tracked rx_reg_dev for rx_ops, the ifindex is intentionally left unchanged for tx_ops. bcm_tx_setup() always rejects ifindex 0, so clearing it would strand the	2026-08-15	7.1	CVE-2026-72116

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	op: neither a later TX_SETUP (bcm_find_op()) nor TX_DELETE (bcm_delete_tx_op()) could ever find it again, since both require an exact ifindex match.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: extend bcm_tx_lock usage for data and timer updates Stage new CAN frame content for an existing tx op into a kmalloc()'d buffer and validate it there, mirroring the approach already used in bcm_rx_setup(). Only copy the validated data into op->frames while holding op->bcm_tx_lock, so bcm_can_tx() and bcm_tx_timeout_handler() can no longer observe a partially updated or unvalidated frame. Add a missing error path for memcpy_from_msg() when copying CAN frame data from userspace. Also move the kt_ival1/kt_ival2/ival1/ival2 updates in bcm_tx_setup() under op->bcm_tx_lock, and read kt_ival1/kt_ival2/count under the same lock in bcm_tx_set_expiry() and bcm_tx_timeout_handler(), closing the torn 64-bit ktime_t read on 32-bit platforms.	2026-08-15	7.8	CVE-2026-72119
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: add missing rcu list annotations and operations sashiko-bot remarked the missing use of list_add_rcu() in bcm_[rx tx]_setup() to have a proper initialized bcm_op structure when bcm_proc_show() traverses the bcm_op's under rcu_read_lock(). To cover all initial settings of the bcm_op's the list_add_rcu() calls are moved to the end of the setup code. While at it, also fix the mirroring removal side: bcm_release() called bcm_remove_op() - which frees the op via call_rcu() - on ops that were still linked in bo->tx_ops/bo->rx_ops, without list_del_rcu() first. Unlink each op with list_del_rcu() before handing it to bcm_remove_op(), matching the existing pattern in bcm_delete_tx_op()/bcm_delete_rx_op().	2026-08-15	7.8	CVE-2026-72120
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: fix lockless bound/ifindex race and silent RX_SETUP failure bcm_sendmsg() reads bo->ifindex and checks bo->bound before taking lock_sock(), while bcm_notify(), bcm_connect() and bcm_release() all mutate both fields under that same lock. Because the lockless reads and the locked writes are unordered with respect to each other, a racing bcm_notify() (device unregister) or bcm_connect() (concurrent bind on another thread sharing the socket) can make bcm_sendmsg() observe an inconsistent combination, e.g. a stale bound=1 together with the now-cleared ifindex=0, silently turning a socket bound to a specific CAN interface into one that also matches "any" interface. Keep the lockless bo->bound check purely as a fast-path reject, and move the ifindex read (and a bo->bound re-check) into the locked section, where every writer already serializes. This removes the possibility of observing the two fields torn against each other, rather than trying to fix it with more READ_ONCE()/WRITE_ONCE() pairs on two independently updated fields. Annotate the now-purely-lockless bo->bound accesses consistently across all its write sites. Also fix bcm_rx_setup() silently returning success when the target device disappears concurrently instead of reporting -ENODEV, so a broken RX op is no longer left registered as if it had succeeded.	2026-08-15	7.3	CVE-2026-72122
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: bcm: defer rx_op deallocation to workqueue to fix thrtimer UAF Commit f1b4e32aca08 ("can: bcm: use call_rcu() instead of costly synchronize_rcu()") replaced synchronize_rcu() in bcm_delete_rx_op() with call_rcu() and introduced the RX_NO_AUTOTIMER flag. However, this flag check was omitted for thrtimer in the packet rx fast-path. During BCM RX operation teardown, a concurrent RCU reader (bcm_rx_handler) can race and re-arm thrtimer via bcm_rx_update_and_send() after call_rcu() has been scheduled. Once the RCU grace period elapses, bcm_op is freed. The subsequently firing thrtimer then dereferences the deallocated op, causing a UAF. Adding flag checks to the rx fast-path (bcm_rx_update_and_send) does not fully close the TOCTOU race and introduces latency for every CAN frame. Conversely, calling hrtimer_cancel() directly inside the RCU callback (softirq context) is fatal as hrtimer_cancel() can sleep, triggering a "scheduling while atomic" panic. Resolve this by deferring the timer cancellation and memory free to a dedicated unbound workqueue (bcm_wq). The RCU callback now queues a work item to bcm_wq, which safely cancels both timers and deallocates memory in sleepable process context. A dedicated workqueue is used to prevent system-wide WQ saturation and is cleanly flushed/destroyed on module unload to avoid rmmio page faults. Since the deferred work can now outlive the calling context by an unbounded amount, also take a reference on op->sk when it is assigned and drop it only once the deferred work has cancelled both timers, so a socket can no longer be freed out from under a still-armed timer whose callback (bcm_send_to_user()) dereferences op->sk.	2026-08-15	7.8	CVE-2026-72123

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: isotp: fix use-after-free race with concurrent NETDEV_UNREGISTER isotp_release() looked up the bound network device via dev_get_by_index() using the stored ifindex. During device unregistration the device is unlisted from the ifindex hash before the NETDEV_UNREGISTER notifier chain runs, so a concurrent isotp_release() could find no device, skip can_rx_unregister() entirely, and still proceed to free the socket. Since isotp_release() had already removed itself from the isotp notifier list at that point, isotp_notify() would never get a chance to clean up either, leaving a stale CAN filter that keeps pointing at the freed socket. Fix this the same way raw.c already does: hold a tracked reference to the bound net_device in the socket (so->dev/so->dev_tracker) from bind() onward instead of re-resolving it from the ifindex, and serialize bind()/release() with rtnl_lock() so that so->dev is always consistent with what the NETDEV_UNREGISTER notifier sees. so->dev stays valid regardless of ifindex-hash unlisting, and is only ever cleared by whichever of isotp_release()/isotp_notify() gets there first, so the filter is always removed exactly once. isotp_bind() now rejects a (re)bind with -EAGAIN while so->[tx rx].state isn't ISOTP_IDLE yet, so a timer left running by a prior NETDEV_UNREGISTER can't act on a newly bound so->ifindex. Both checks share the same lock_sock() section, so there is no window in which a concurrent isotp_notify() clearing so->bound could be missed.	2026-08-15	7.8	CVE-2026-72125
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: isotp: use unconditional synchronize_rcu() in isotp_release() isotp_notify() unregisters the (RCU) CAN filters via can_rx_unregister() and clears so->bound without waiting for a grace period. isotp_release() uses so->bound to decide whether it needs to call synchronize_rcu() before cancelling so->rxtimer, so when NETDEV_UNREGISTER runs first it skips that synchronize_rcu() and can cancel the timer while an in-flight isotp_rcv() is still executing and about to re-arm it via isotp_send_fc(), leading to a use-after-free timer callback on the freed socket. sakisho-bot remarked a problem with rtnl_lock held in isotp_notify(), therefore make isotp_release() always call synchronize_rcu() before cancelling the timers, regardless of so->bound. This still closes the original race (isotp_notify() clearing so->bound without waiting for in-flight isotp_rcv() callers before isotp_release() cancels the RX timer) without adding any RCU wait to the netdevice notifier path.	2026-08-15	7.8	CVE-2026-72126
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: spi: imx: reconfigure for PIO when DMA cannot be started When spi_imx_can_dma() selects DMA, the ECSPI is configured for DMA: spi_imx_setupxfer() sets CTRL.SMC and clears dynamic_burst, and spi_imx_dma_transfer() programs the dynamic-burst BURST_LENGTH and the SDMA watermarks. If the DMA descriptor cannot be prepared (dmaengine_prep_slave_single() returns NULL), the transfer is failed with SPI_TRANS_FAIL_NO_START and falls back to PIO. The dynamic-burst DMA path uses its own bounce buffers instead of the SPI core's mapping, so xfer->[tx,rx].sg_mapped are not set and the core's DMA->PIO retry is skipped; the driver falls back to PIO internally. But none of the DMA-mode configuration is undone, so the PIO transfer runs with CTRL.SMC set, the wrong burst length and dynamic_burst cleared, and the transferred data is corrupted. This is easily hit on i.MX8MP boards that describe ECSPI DMA in the device tree but run SDMA on i.MX8MP firmware (no external sdma-imx7d.bin): every ECSPI DMA prepare fails. An Infineon SLB9670 TPM on ECSPI1 then returns shifted TPM2_GetCapability data, is flagged "field failure mode", /dev/tpmrm0 is never created. Set controller->fallback before re-running spi_imx_setupxfer() so the ECSPI is reconfigured exactly like a normal PIO transfer. With controller->fallback set, spi_imx_setupxfer() sees spi_imx_can_dma() return false, so it clears spi_imx->usedma and reprograms the controller (clears CTRL.SMC, restores dynamic_burst and the PIO burst length). No explicit spi_imx->usedma = false is needed: setupxfer() already updates it from the can_dma() result.	2026-08-15	7.8	CVE-2026-72134
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tpm: Make the TPM character devices non-seekable The TPM character devices expose a sequential command/response interface, but their open handlers leave FMODE_PREAD and FMODE_PWRITE enabled. After a command leaves a response pending, pread(fd, buf, 16, 0x1400) passes 0x1400 as *off to tpm_common_read(). The transfer length is bounded by response_length, but the offset is used unchecked when forming data_buffer + *off. A sufficiently large offset therefore causes an out-of-bounds heap read through copy_to_user() and, if the copy succeeds, an out-of-bounds zero-write through the following memset(). Positional I/O does not provide coherent semantics for this interface. An arbitrary pread	2026-08-15	7.8	CVE-2026-72135

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	offset cannot represent how much of a response has been consumed sequentially. The write callback always stores a command at the start of data_buffer, while pwrite() does not update file->f_pos and can leave the sequential read cursor stale. Call nonseekable_open() from both open handlers. This removes FMODE_PREAD and FMODE_PWRITE, causing positional reads and writes to fail with -ESPIPE before reaching the TPM callbacks, and explicitly marks the files non-seekable. Normal read() and write() continue to use the existing sequential f_pos cursor, leaving the response state machine unchanged. Tested on Linux 6.12 with KASAN and a swtpm TPM2 device: - sequential partial reads returned the complete response - pread() and preadv() with offset 0x1400 returned -ESPIPE - pwrite() and pwritev() with offset zero returned -ESPIPE - the pending response remained intact after the rejected operations - a subsequent normal command/response cycle completed normally - no KASAN report was produced.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: i2c: imx: fix locked bus on SMBus block-read of 0 (IRQ) SMBus 3.1 6.5.7 allows a Block Read byte count of 0, but the interrupt-driven block-read state machine rejects it as -EPROTO. Worse, it returns without a NACK+STOP: the next receive cycle has already started, so the target keeps holding SDA and the bus stays stuck until a power cycle of this i2c controller. Accept count=0: NACK the in-flight dummy byte (TXAK) and set msg->len to 2 so i2c_imx_isr_read_continue() emits STOP via its normal last-byte path. The dummy byte is discarded; block-read callers only consume buff[0..count-1]. Reading I2DR has likewise already armed the next byte on the count > I2C_SMBUS_BLOCK_MAX error path, so NACK it (TXAK) before aborting with -EPROTO; otherwise the failing transfer's STOP cannot complete and the bus stays held. The atomic path regressed earlier (v3.16) and is fixed separately; this patch covers only the v6.13 state-machine rework.	2026-08-15	7.5	CVE-2026-72141
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: platform/x86: ISST: Restore SST-PP control to all domains The SST-PP control offset is only restored to power domain 0 after resume. During suspend, control values are read and stored for all power domains. Use pd_info->sst_base instead of power_domain_info->sst_base, which only points to power domain 0 base address.	2026-08-15	7.1	CVE-2026-72143
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: platform/x86: dell-laptop: fix missing cleanups in init error path dell_init() initializes several resources after dell_setup_rfkil(), including the optional touchpad LED, keyboard backlight LED, battery hook, debugfs directory and dell-laptop notifier. If a later LED or backlight registration fails, the error path only tears down the battery hook and rfkill resources. This leaves the notifier, debugfs directory, keyboard backlight LED and optional touchpad LED registered after dell_init() returns an error. Add the missing cleanup calls before tearing down rfkill.	2026-08-15	7.8	CVE-2026-72144
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dmaengine: tegra: Fix burst size calculation Currently, the Tegra GPC DMA hardware requires the transfer length to be a multiple of the max burst size configured for the channel. When a client requests a transfer where the length is not evenly divisible by the configured max burst size, the DMA hangs with partial burst at the end. Fix this by reducing the burst size to the largest power-of-2 value that evenly divides the transfer length. For example, a 40-byte transfer with a 16-byte max burst will now use an 8-byte burst (40 / 8 = 5 complete bursts) instead of causing a hang. This issue was observed with the PL011 UART driver where TX DMA transfers of arbitrary lengths were stuck.	2026-08-15	7.5	CVE-2026-72149
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: openrisc: Fix jump_label smp syncing The original commit 8c30b0018f9d ("openrisc: Add jump label support") copies from arm64 and does not properly consider how icache invalidation on remote cores works in OpenRISC. On OpenRISC remote icaches need to be invalidated otherwise static key's may remain state after updating. Fix SMP cache syncing by: 1. Properly invalidate remote core icaches on SMP systems by using icache_all_inv. The old code uses kick_all_cpus_sync() which runs a no-op IPI function call on remote CPU's which does execute a lot of code and flushes many cache lines in the process, but does not flush all and it's not correct on OpenRISC. 2. For architectures that do not have WRITETHROUGH caches be sure to flush the dcache after patching. To test this I first reproduced the issue using a custom test module [0]. The test confirmed that some icache lines maintained stale static_key code sequences after calling static_branch_enable(). After this patch there are no longer jump_label coherency issues. [0] https://github.com/stffrdhrn/or1k-utils/tree/master/tests/smp_static_key_test	2026-08-15	7.8	CVE-2026-72154

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix UBSAN array-index-out-of-bounds in ocfs2_sum_rightmost_rec [BUG] On-disk corruption setting l_next_free_rec to 0 in an inode's embedded extent list triggers a UBSAN panic on the next write to that file. [CAUSE] ocfs2_sum_rightmost_rec() computes i = le16_to_cpu(el->l_next_free_rec) - 1 and accesses el->l_recs[i] without validating i. When l_next_free_rec is 0, i becomes -1; when l_next_free_rec exceeds l_count, i falls past the end of the array. Either case violates the __counted_by_le(l_count) annotation on l_recs[] and triggers UBSAN. [FIX] Validate the inode's embedded extent list when the inode is read, in ocfs2_validate_inode_block(): l_count must be non-zero and no larger than the inode block can hold, and l_next_free_rec must not exceed l_count. A corrupt list is rejected at read time, before the b-tree code can index l_recs[] out of bounds.	2026-08-15	7.8	CVE-2026-72162
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: avoid moving extents to occupied clusters For non-auto OCFS2_IOC_MOVE_EXT operations, userspace supplies a physical me_goal. ocfs2_move_extent() initializes new_phys_cpos from that goal and expects ocfs2_probe_alloc_group() to replace it with a free run in the target block group. The probe currently leaves *phys_cpos unchanged if the scan reaches the end of the group without finding a free run. An occupied goal at the last bit can therefore survive the probe and be passed to __ocfs2_move_extent(), which copies file data into a cluster still owned by another inode before the bitmap is updated. When the probe does find a free run, it also subtracts move_len from the ending bit. The start of an N-bit run ending at i is i - N + 1, so the current calculation can report the bit immediately before the free run. Clear *phys_cpos before scanning and use the correct free-run start. Callers already treat a zero result as -ENOSPC, so failed probes no longer continue with an occupied caller-controlled goal.	2026-08-15	7.8	CVE-2026-72164
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix condition in 'nand_select_target()' 'cs' here must be in range [0:nanddev_ntargets[.	2026-08-15	7.8	CVE-2026-72165
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: 9p: skip nlink update in cacheless mode to fix WARN_ON v9fs_dec_count() unconditionally calls drop_nlink() on regular files, even when the inode's nlink is already zero. In cacheless mode the client refetches inode metadata from the server (the source of truth) on every operation, so by the time v9fs_remove() returns, the locally cached nlink may already reflect the post-unlink value: 1. Client initiates unlink, server processes it and sets nlink to 0 2. Client refetches inode metadata (nlink=0) before unlink returns 3. Client's v9fs_remove() completes successfully 4. Client calls v9fs_dec_count() which calls drop_nlink() on nlink=0 This race is easily triggered under heavy unlink workloads, such as stress-ng's unlink stressor, producing the following warning: WARNING: fs/inode.c:417 at drop_nlink+0x4c/0xc8 Call trace: drop_nlink+0x4c/0xc8 v9fs_remove+0x1e0/0x250 [9p] v9fs_vfs_unlink+0x20/0x38 [9p] vfs_unlink+0x13c/0x258 ... In cacheless mode the server is authoritative and the inode is on its way out, so locally adjusting nlink buys nothing. Skip v9fs_dec_count() entirely when neither CACHE_META nor CACHE_LOOSE is set, which both avoids the warning and removes a class of nlink races (two concurrent unlinkers observing nlink > 0 and both calling drop_nlink()) that an nlink == 0 guard alone would only narrow rather than close.	2026-08-15	7.8	CVE-2026-72170
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mtd: slram: remove failed entries from the device list register_device() links a new slram_mtdlist entry before allocating all of the state needed by the entry. If a later allocation, memremap(), or mtd_device_register() fails, the partially initialized entry remains on the global list. A later cleanup can then dereference or free invalid state from that failed entry. Unwind the partially initialized entry and clear the list tail on each failure path after the entry has been linked.	2026-08-15	7.8	CVE-2026-72171
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/mm_init: fix uninitialized struct pages for ZONE_DEVICE If DAX memory is hotplugged into an unoccupied subsection of an early section, section_activate() reuses the unoptimized boot memmap. However, compound_nr_pages() still assumes that vmemmap optimization is in effect and initializes only the reduced number of struct pages. As a result, the remaining tail struct pages are left uninitialized, which can later lead to unexpected behavior or crashes. Fix this by treating early sections as unoptimized when calculating how many struct pages to initialize.	2026-08-15	7.8	CVE-2026-72172
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mm: fix make_uffd_wp_huge_pte() prot-update race Patch series "userfaultfd/pagemap: pre-existing fixes". These are pre-existing bug fixes that	2026-08-15	7.1	CVE-2026-72175

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	were carried at the front of the userfaultfd RWP working-set-tracking series up to v5 [1]. Per review feedback that fixes should not sit in the middle of a feature series, they are split out and sent on their own; the RWP series is reposted rebased on top of this. All six were flagged by the Sashiko AI review of the RWP series and carry independent of RWP, apply to mm-new directly, and carry Cc: stable@. 1: fs/proc/task_mmu: a missing huge_ptep_modify_prot_start() in make_uffd_wp_huge_pte() can lose hardware Dirty/Accessed updates when PAGESCAN_SCAN write-protects a hugetlb PTE. 2: fs/proc/task_mmu: pagemap_scan_hugetlb_entry() compares the range against HPAGE_SIZE rather than the hstate page size, so it never write-protects gigantic hugetlb pages. 3: fs/proc/task_mmu: PAGESCAN_SCAN with PM_SCAN_WP_MATCHING over an unpopulated hugetlb range self-deadlocks -- pagemap_scan_pte_hole() calls uffd_wp_range() while walk_hugetlb_range() holds the hugetlb vma lock for read, and hugetlb_change_protection() then takes it for write. Install the marker inline instead. 4: mm/huge_memory: change_non_present_huge_pmd() drops pmd_swp_uffd_wp on a device-private PMD permission downgrade, silently losing the uffd-wp marker. 5: userfaultfd: must_wait() applies pte_write() to a locklessly read PTE without checking pte_present(), so swap/migration entries decode random offset bits and a thread can stay parked on a stale fault. 6: userfaultfd: __VMA_UFFD_FLAGS feeds VMA_UFFD_MINOR_BIT (41) to mk_vma_flags() unconditionally, an out-of-bounds write into the single-word vma_flags_t on 32-bit. Build the mask from config-gated per-mode masks so an unavailable bit is never materialised. This patch (of 6): make_uffd_wp_huge_pte() arms the UFFD_WP bit on a present HugeTLB PTE by calling huge_ptep_modify_prot_commit() with a pte snapshot that was fetched without the corresponding huge_ptep_modify_prot_start(). The start helper is what atomically clears the entry so the kernel-owned snapshot stays consistent until the commit; without it, the hardware may set Dirty or Accessed in the live PTE between the original read and the commit, and huge_ptep_modify_prot_commit() (whose generic implementation just calls set_huge_pte_at()) then writes the stale snapshot back over the live hardware bits, losing the update. The non-hugetlb sibling make_uffd_wp_pte() does this correctly via ptep_modify_prot_start() / ptep_modify_prot_commit(). Mirror that pattern for the present-PTE branch. The migration case stays as-is -- migration entries are non-present, so there's no hardware update to race against.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mips: sched: Fix CPUMASK_OFFSTACK memory corruption This patch addresses a critical memory management flaw. When CONFIG_CPUMASK_OFFSTACK is enabled, cpumask_var_t is a pointer. Consequently, sizeof(new_mask) evaluates to the pointer size, causing copy_from_user() to clobber the mask pointer. Furthermore, the old logic performed copy_from_user() before allocating the mask. Fix this by allocating new_mask first. To handle variable-sized user masks correctly, use cpumask_size() to truncate overly large user masks or pad undersized masks with zeros before copying the data directly into the allocated buffer.	2026-08-15	7.8	CVE-2026-72181
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: bound attr_off in UpdateResidentValue against data_off In do_action()'s UpdateResidentValue case (fslog.c:3307), lrh->attr_off and lrh->redo_len come from the on-disk LRH. When they satisfy aoff + dlen < attr->res.data_off, the assignment attr->res.data_size = cpu_to_le32(aoff + dlen - data_off); underflows to ~4 GiB (e.g. 0xFFFFFFFF9 when aoff=0x10, dlen=1, data_off=0x18). Subsequent code that reads attr->res.data_size to walk the resident attribute payload would then read up to 4 GiB past the 1024-byte MFT record allocation. The existing mi_enum_attr() defense in fs/ntfs3/record.c:287 catches the corrupted data_size on the next attribute walk and fails the mount, but only on the path that walks all attributes. A read site that picks an attribute by name and reads its data_size without re-validating is not covered. Validate aoff against data_off and asize at the source. Reproduced under UML+KASAN on mainline 8d90b09e6741 via pr_warn-only probe: with aoff=0x10 and data_off=0x18, the post-assignment data_size is 0xffffffff9 (mount then fails at -22 from mi_enum_attr). [almaz.alexandrovich@paragon-software.com: clang-formatted the changes]	2026-08-15	7.8	CVE-2026-72195
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: reject non-resident records for resident-only attributes The shared lookup-time attribute validator rejects non-resident \$FILE_NAME and \$VOLUME_NAME records because their formats require resident values and callers handle returned records as resident attributes. Other resident-only attribute types still pass through the	2026-08-15	7.8	CVE-2026-72198

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	generic non-resident mapping-pairs checks. That leaves real resident/non-resident union confusion paths. Inode load looks up \$STANDARD_INFORMATION and then reads data.resident.value_offset without checking a->non_resident. ntfs_inode_sync_standard_information() does the same when updating the standard information value. ntfs_write_volume_flags() also looks up \$VOLUME_INFORMATION and reads data.resident.value_offset directly. \$INDEX_ROOT callers in dir.c and index.c depend on the same lookup contract before consuming the resident index root value. Reject non-resident records for all resident-only attribute types in the shared validator. Keep the existing \$FILE_NAME and \$VOLUME_NAME behavior, but factor it through a helper and extend it to \$STANDARD_INFORMATION, \$OBJECT_ID, \$VOLUME_INFORMATION, \$INDEX_ROOT, and \$EA_INFORMATION. For \$OBJECT_ID and \$EA_INFORMATION this is contract hardening for resident-only formats; this patch only rejects the non-resident form and does not add new resident value validation for those types.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: avoid heap allocation for free-cluster readahead state get_nr_free_clusters() allocates a temporary file_ra_state before it publishes the precomputed free cluster count, sets NVolFreeClusterKnown(), and wakes vol->free_waitq. If that allocation fails, the worker returns without setting the flag or waking waiters, so callers waiting for the free count can block indefinitely. The readahead state is only used synchronously while scanning the bitmap. Keep it on the stack and pass it by address to the readahead helper. This eliminates the early allocation failure path instead of adding a special case that publishes a conservative count and wakes the waitqueue. Zero-initialize the on-stack state because file_ra_state_init() only sets ra_pages and prev_pos. Apply the same treatment to __get_nr_free_mft_records(), which scans the MFT bitmap with the same short-lived readahead state.	2026-08-15	7.5	CVE-2026-72202
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: skip extent mft records in writeback to prevent deadlock This patch fixes the ABBA deadlock between extent_lock and extent mrec_lock triggered by xfstests generic/113, that occurs since the commit 6994acf33bae ("ntfs: use base mft_no when looking up base inode for extent record"). Path A (inode writeback): VFS writeback -> ntfs_write_inode() -> __ntfs_write_inode() -> mutex_lock(&ni->extent_lock) -> mutex_lock(&tni->mrec_lock) Path B (MFT folio writeback): VFS writeback of \$MFT dirty folios -> ntfs_mft_writepages() -> ntfs_write_mft_block() -> ntfs_may_write_mft_record() -> holds one extent mrec_lock from a previous iteration -> tries to acquire another base inode extent_lock By removing all extent_lock and extent mrec_lock acquisition from the MFT folio writeback path, the ABBA lock ordering is eliminated: Path A: __ntfs_write_inode(): extent_lock -> mrec_lock Path B (removed): ntfs_write_mft_block(): mrec_lock -> extent_lock Path B is always redundant for extent records because: 1. mark_mft_record_dirty(ext_ni) does NOT dirty the MFT folio. It only sets NiNoDirty(ext_ni) and marks the base VFS inode dirty via __mark_inode_dirty(I_DIRTY_DATASYNC), which triggers Path A. Therefore, normal extent modifications never create a situation where the MFT folio is dirty and Path B is not scheduled. 2. The MFT folio only gets dirtied via ntfs_mft_mark_dirty() inside ntfs_mft_record_alloc(). But all identified callers in attrib.c (ntfs_attr_add, ntfs_attr_record_move_away, ntfs_attr_make_non_resident, ntfs_attr_record_resize) follow through with mark_mft_record_dirty(), which triggers Path A to write the complete record. 3. ntfs_evict_big_inode() calls ntfs_commit_inode() before freeing extent inodes, ensuring all dirty extents are flushed via Path A before the base inode leaves the icache.	2026-08-15	7.5	CVE-2026-72203
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix hugetlb cgroup rsvd charge/uncharge mismatch In alloc_hugetlb_folio(), a single h_cg pointer is used for both the rsvd and non-rsvd hugetlb cgroup charges. When map_chg is set, hugetlb_cgroup_charge_cgroup_rsvd() stores the charged cgroup in h_cg, but the immediately following hugetlb_cgroup_charge_cgroup() overwrites h_cg with the non-rsvd cgroup pointer. As a result, hugetlb_cgroup_commit_charge_rsvd() stores the wrong (non-rsvd) cgroup pointer into the folio's rsvd slot. When the folio is later freed, free_huge_folio() unconditionally calls both hugetlb_cgroup_uncharge_folio() and hugetlb_cgroup_uncharge_folio_rsvd(). The rsvd uncharge reads back the wrong cgroup from the folio and decrements a counter that was never charged for that cgroup, causing a page_counter underflow: page_counter underflow: -512 nr_pages=512 WARNING: mm/page_counter.c:61 at page_counter_cancel Fix this	2026-08-15	7.1	CVE-2026-72213

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by introducing a separate h_cg_rsvd pointer exclusively for the rsvd charge path, keeping the rsvd and non-rsvd charges fully independent through their charge, commit, and error uncharge paths.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: jbd2: fix integer underflow in jbd2_journal_initialize_fast_commit() jbd2_journal_initialize_fast_commit() validates journal capacity by checking (journal->j_last - num_fc_blks < JBD2_MIN_JOURNAL_BLOCKS). Both j_last and num_fc_blks are unsigned, so when num_fc_blks exceeds j_last the subtraction wraps to a large value, bypassing the bounds check. The resulting underflow corrupts j_last, j_fc_first, and j_free, leading to journal abort. Fix by checking num_fc_blks against j_last before the subtraction, returning -EFSCORRUPTED.	2026-08-15	7.8	CVE-2026-72225
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: tt: avoid request storms during pending request batadv_send_tt_request() allocates a tt_req_node when none exists for the destination originator node. This should prevent that a multiple TT requests are send at the same time to an originator. But if allocation of the send buffer failed, this request must be cleaned up again. But indicator for such a failure is "ret == false". But the actual implementation is checking for "ret == true". The check must be inverted to not loose the information about the TT request directly after it was attempted to be sent out. This should avoid potential request storms.	2026-08-15	7.5	CVE-2026-72231
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: ensure minimal ethernet header on TX As documented in commit 8bd67ebb50c0 ("net: bridge: xmit: make sure we have at least eth header len bytes"), it is possible by for a local user with eBPF TC hook access to attach a tc filter which truncates the packet and redirects to an batadv interface. But the code assumes that at least ETH_HLEN bytes are available and thus might read outside of the available buffer. The batadv_interface_tx() must therefore always check itself if enough data is available for the ethernet header and don't rely on min_header_len.	2026-08-15	7.8	CVE-2026-72232
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: selinux: avoid sk_socket dereference in selinux_sctp_bind_connect() selinux_sctp_bind_connect() dereferences sk->sk_socket to pass a struct socket * to selinux_socket_bind() and selinux_socket_connect_helper(). However, when the hook is invoked from the ASCONF softirq path (sctp_process_asconf), there is no file reference guaranteeing that sk->sk_socket is non-NULL. The setsockopt callers (bindx, connectx, set_primary, sendmsg connect) hold a file reference and are not affected. Both selinux_socket_bind() and selinux_socket_connect_helper() immediately resolve sock->sk, never using the struct socket * for anything else. Refactor the inner logic into helpers that take a struct sock * directly so that selinux_sctp_bind_connect() never needs to touch sk->sk_socket at all.	2026-08-15	7.5	CVE-2026-72242
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gpu/buddy: bail out of try_harder when alignment cannot be honoured The try_harder contiguous fallback could return a range whose start offset did not match the caller's min_block_size. When a candidate's start is misaligned, realign it: free the misaligned run and reallocate exactly @size at the next lower min_block_size boundary. This keeps the returned size unchanged with no surplus to trim, and rejects the request only when no aligned candidate fits. v2: align misaligned candidates down to min_block_size instead of bailing out, for both the RHS and LHS paths (Matthew).	2026-08-15	7.8	CVE-2026-72244
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conncount: fix zone comparison in tuple dedup The "already exists" dedup logic in __nf_conncount_add() decides whether a connection has already been counted and can be skipped instead of incrementing the connlimit count. It compares the conntrack zone of a list entry with the zone of the connection being added using nf_ct_zone_id() and nf_ct_zone_equal(), passing conn->zone.dir or zone->dir as the direction argument. Those helpers take enum ip_conntrack_dir values: IP_CT_DIR_ORIGINAL is 0 and IP_CT_DIR_REPLY is 1. However, zone->dir is a u8 bitmask: NF_CT_ZONE_DIR_ORIG is 1, NF_CT_ZONE_DIR_REPL is 2 and NF_CT_DEFAULT_ZONE_DIR is 3. Passing that bitmask as the enum direction shifts the meaning of every non-zero value. An ORIG-only zone passes 1 and is tested as REPLY, while REPL-only and default zones pass 2 or 3 and test bits beyond the valid direction range. In those cases nf_ct_zone_id() can fall back to NF_CT_DEFAULT_ZONE_ID instead of using the real zone id, so different zones can be treated as equal and dedup collapses to tuple equality alone. nf_conncount stores and compares the original-direction tuple for a connection. If an skb already	2026-08-15	7.5	CVE-2026-72247

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	has an attached conntrack entry, get_ct_or_tuple_from_skb() explicitly copies ct->tuplehash[IP_CT_DIR_ORIGINAL].tuple, regardless of the packet's ctinfo. Therefore the zone comparison in the tuple dedup path must use IP_CT_DIR_ORIGINAL as well; the zone direction bitmask describes where a zone id applies, not which direction this conncount tuple represents. Fix the two dedup comparisons by passing IP_CT_DIR_ORIGINAL directly. Do not special-case NF_CT_DEFAULT_ZONE_DIR and do not compare raw zone ids: using the existing helpers with IP_CT_DIR_ORIGINAL preserves the direction-aware NF_CT_DEFAULT_ZONE_ID fallback. A default bidirectional zone contains the ORIG bit, so it naturally returns the real zone id; reply-only zones continue to fall back for original-direction tuple comparisons.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_reasm: guard mac_header adjustment after IPv6 defrag nf_ct_frag6_reasm() slides the packet head forward to drop the IPv6 fragment header and then unconditionally advances skb->mac_header: skb->mac_header += sizeof(struct frag_hdr); On the NF_INET_LOCAL_OUT defrag path the skb has no link-layer header yet, so skb->mac_header is still the "not set" sentinel (u16)~0U. Adding sizeof(struct frag_hdr) wraps it to a small value (0xffff + 8 == 7), after which skb_mac_header_was_set() wrongly reports a MAC header is present and skb_mac_header() points into the headroom. The reassembler has done this unconditional add since it was introduced; it was harmless while mac_header was a bare pointer, but wrong once mac_header became a u16 offset whose unset state is the ~0U sentinel tested by skb_mac_header_was_set(). The sibling net/ipv6/reassembly.c does the same relocation and does guard the adjustment; mirror the guard here.	2026-08-15	7.8	CVE-2026-72250
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_pipapo: don't leak bad clone into future transaction On memory allocation failure the cloned nft_pipapo_match can enter a bad state: - some fields can have their lookup tables resized while others did not - bits might have been toggled - scratch map can be undersized which also means m->bsize_max can be lower than what is required This means that the next insertion in the same batch can trigger out-of-bounds writes. Furthermore, a failure in the first can result in the bad clone to leak into the next transaction because the abort callback is never executed in this case (the upper layer saw an error and no attempt to allocate a transactional request was made). Record a state for the nft_pipapo_match structure: - NEW (pristine clone) - MOD (modified clone with good state) - ERR (potentially bogus content) Then make it so that deletes and insertions fail when the clone entered ERR state. In case the very first insert attempt results in an error, free the clone right away.	2026-08-15	7.8	CVE-2026-72252
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_sip: validate skb_dst() before accessing it tc ingress and openvswitch do not guarantee routing information to be available. These subsystems use the conntrack helper infrastructure, and the SIP helper relies on the skb_dst() to be present if sip_external_media is set to 1 (which is disabled by default as a module parameter). This effectively disables the sip_external_media toggle for these subsystems without resulting in a crash.	2026-08-15	7.5	CVE-2026-72253
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_fib: reject fib expression on the netdev egress hook A fib expression in a netdev egress base chain dereferences nft_in(pkt), NULL on the transmit path, causing a NULL pointer dereference at eval. nft_fib_validate() masks the hook with NF_INET_* values, but netdev hook numbers are a separate enum that aliases them (NF_NETDEV_EGRESS == NF_INET_LOCAL_IN), so an egress chain passes validation and then faults. Add nft_fib_netdev_validate() that limits each result/flag to the netdev hook where the device it reads exists: the input-device cases (OIF, OIFNAME, ADDRTYPE with F_IIF) to ingress, the output-device case (ADDRTYPE with F_OIF) to egress, ADDRTYPE with no device flag to both. Also restrict nft_fib_validate() to NFPROTO_IPV4/IPV6/INET so its NF_INET_* masks are not applied to another family's hooks.	2026-08-15	7.5	CVE-2026-72254
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_queue: pin bridge device while NFQUEUE holds fake dst The br_netfilter fake table is embedded in struct net_bridge and is attached to bridged packets with skb_dst_set_noref(). If such a packet is queued to NFQUEUE, __nf_queue() upgrades that fake dst with skb_dst_force(). At that point the queued skb can hold a real dst reference after bridge teardown has started. The problem is not that every bridged packet needs its own dst reference. The problem is that NFQUEUE	2026-08-15	7.8	CVE-2026-72255

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can keep the bridge private fake dst alive after unregister begins. Fix this by keeping the bridge fake dst model unchanged and pinning the bridge master device only while the packet sits in NFQUEUE. Record the bridge device in nf_queue_entry when the queued skb carries a bridge fake dst, take a device reference for the queue lifetime, and drop it when the queue entry is freed. Also make sure queued entries are reaped when that bridge device goes down, and drop the redundant nf_bridge_info_exists() test from the fake dst detection. This keeps netdev_priv(br->dev) alive until verdict completion, so the embedded fake rtable and its metrics backing storage cannot be freed out from under dst_release(). It also avoids the constant refcount bump and avoids using ipv4-specific dst helpers for IPv6 bridge traffic.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc3-control: Validate size in snd_sof_update_control In snd_sof_update_control(), firmware-provided cdata->num_elems is checked against local_cdata->data->size but never against the actual allocation size. If local_cdata->data->size was previously set to an inconsistent value, the memcpy could write past the allocated buffer. Add a bounds check to ensure num_elems fits within the available space in the ipc_control_data allocation before copying.	2026-08-15	7.8	CVE-2026-72261
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc3-control: Fix heap overflow in bytes_ext put/get The ipc_control_data buffer is allocated as kzalloc(max_size), where max_size covers the entire struct sof_ipc_ctrl_data including its flexible array payload. However, the bounds checks in bytes_ext_put and _bytes_ext_get compared user data lengths against max_size directly, ignoring that cdata->data sits at an offset of sizeof(struct sof_ipc_ctrl_data) bytes into the allocation. This allowed writing up to sizeof(struct sof_ipc_ctrl_data) bytes past the end of the heap buffer from unprivileged userspace via the ALSA TLV kcontrol interface, and similarly allowed over-reading adjacent heap data on the get path. Fix all bounds checks to subtract sizeof(*cdata) from max_size so they reflect the actual space available at the cdata->data offset. Also fix the error-path restore in bytes_ext_put which wrote to cdata->data instead of cdata, causing the same overflow.	2026-08-15	7.8	CVE-2026-72262
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Drop bogus WARN for write to ZCR_EL2 It is entirely possible for a guest to write to the ZCR_EL2 sysreg alias while in a nested context, as it is expected if FEAT_NV2 is advertised to the L1 hypervisor. Get rid of the bogus WARN which, since the hyp vectors were installed at this point, has the effect of a hyp_panic...	2026-08-15	7.1	CVE-2026-72280
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: Move kvm_io_bus_get_dev() locking responsibilities to callers kvm_io_bus_get_dev() returns a device that is only matched by the address, and nothing else. This can cause a lifetime issue if the matched device is not the expected type, as by the time the caller can introspect the object, it might be gone (the srcu lock having been dropped). Given that there is only a single user of this helper, the simplest option is to move the locking responsibility to the caller, which can keep the srcu lock held for as long as it wants. Note that this aligns with other kvm_io_bus*() helpers, which already require the srcu lock to be held by the callers.	2026-08-15	7.8	CVE-2026-72282
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Ignore pending PV EOI if the vCPU has since disabled PV EOIs Ignore KVM's internal "service pending PV EOI" request if the vCPU has disabled PV EOIs since the request was made. Asserting that PV EOIs are enabled can fail if reading guest memory in pv_eoi_get_user() fails, i.e. if pv_eoi_test_and_clr_pending() bails early, *and* the vCPU also disables PV EOIs. kernel BUG at arch/x86/kvm/lapic.c:3338! Oops: invalid opcode: 0000 [#1] SMP CPU: 4 UID: 1000 PID: 890 Comm: pv_eoi_test Not tainted 7.0.0-d585aa5894d8-vm #337 PREEMPT Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 RIP: 0010:kvm_lapic_sync_from_vapic+0x12b/0x140 [kvm] Call Trace: <TASK> kvm_arch_vcpu_ioctl_run+0x1075/0x1c30 [kvm] kvm_vcpu_ioctl+0x2d5/0x980 [kvm] __x64_sys_ioctl+0x8a/0xd0 do_syscall_64+0xb5/0xb40 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK> Modules linked in: kvm_intel kvm irqbypass ---[end trace 0000000000000000]---	2026-08-15	7.1	CVE-2026-72284
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: TDX: Reject concurrent change to CPUID entry count Reject KVM_TDX_INIT_VM if userspace changes cpuid.nent between the initial read and the subsequent copy of the initialization data. tdx_td_init() first reads user_data->cpuid.nent to size the flexible kvm_tdx_init_vm copy. The copied structure also contains cpuid.nent, and	2026-08-15	7.8	CVE-2026-72285

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that field can differ from the value used to size the allocation if userspace modifies the input concurrently. setup_tdpairs_cpuids() later passes init_vm->cpuid.nent to kvm_find_cpuid_entry2(), which uses it as the array bound for the copied entries. Require the copied count to match the value used to size the allocation so that CPUID parsing cannot access beyond the entries actually copied.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: nVMX: Move vTPR vs. TPR Threshold consistency check into "normal" checks Move the off-by-default consistency check for vmcs12.tpr_threshold vs. the virtual APIC vTPR into the "normal" controls checks, as waiting until KVM has loaded some amount of state is unnecessary and actively dangerous. Specifically, failure to unwind vmcs01.GUEST_CR3 to KVM's value when EPT is disabled results in KVM running L1 with an L1-controlled CR3, not with KVM's CR3! Alternatively, KVM could simply reset the MMU to force a reload of vmcs01.GUEST_CR3, but the _only_ reason the check was shoved into a "late" flow was to wait until the vmcs12 pages were retrieved. Rather than build up more crusty code, simply access vTPR using a regular guest memory access (performance isn't a concern). To circumvent the restrictions that led to KVM deferring nested_get_vmcs12_pages(), (a) use a VM-scoped API to read guest memory so that it always hits non-SMM memslots (for RSM), and (b) skip the check (since its off-by-default anyways) when the vCPU doesn't want to run, i.e. when userspace is restoring/stuffing state. If reading guest memory fails, simply skip the consistency check, as KVM's de facto ABI is that VMX instruction accesses to non-existent memory get PCI Bus Error semantics, where reads return 0xFFs. And if vTPR=0xFF, then the vTPR is guaranteed to be greater than or equal to TPR_THRESHOLD.	2026-08-15	7.8	CVE-2026-72287
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: atm: reject out-of-range traffic classes in QoS validation Reject ATM traffic classes above ATM_ANYCLASS in check_tp(). SO_ATMQOS stores the supplied QoS after check_qos() succeeds, so accepting larger values leaves invalid traffic_class values in vcc->qos. That bad state later reaches pvc_info(), which indexes class_name[] with vcc->qos.{rx,tp}.traffic_class. Values above ATM_ANYCLASS cause an out-of-bounds read when /proc/net/atm/pvc is read. Tighten the existing QoS validation so invalid traffic_class values are rejected at the point where user supplied QoS is accepted.	2026-08-15	7.1	CVE-2026-72297
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc3-control: Fix TOCTOU in bytes_put and bytes_get In sof_ipc3_bytes_put(), the size used for the memcpy is derived from the old data->size already in the buffer, not the incoming new data's size field. If the new data has a different size, the copy length is wrong: it may truncate valid data or copy stale bytes. Similarly, sof_ipc3_bytes_get() checks data->size against max_size without accounting for the sizeof(struct sof_ipc_ctrl_data) offset of the flex array within the allocation. Fix bytes_put to validate and use the incoming data's sof_abi_hdr.size from ucontrol before copying. Fix bytes_get to subtract sizeof(*cdata) from the bounds check to match the actual available space.	2026-08-15	7.8	CVE-2026-72301
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc3-control: Use overflow checks in control_update size calc In sof_ipc3_control_update(), the expected_size calculation uses firmware-provided cdata->num_elems in arithmetic that could overflow on 32-bit platforms, wrapping to a small value. This would allow the cdata->rhdr.hdr.size comparison to pass with mismatched sizes, potentially leading to out-of-bounds access in snd_sof_update_control. Use check_mul_overflow() and check_add_overflow() to detect and reject overflowed size calculations.	2026-08-15	7.8	CVE-2026-72302
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-control: Validate notification payload size Validate MODULE_NOTIFICATION payload length before reading bytes/channel data in control update handling.	2026-08-15	7.8	CVE-2026-72303
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: ipc4-control: Fix TOCTOU in sof_ipc4_bytes_put In sof_ipc4_bytes_put(), the copy size is derived from the old data->size in the buffer rather than the incoming new data's size field from ucontrol. If the new data has a different size, the copy uses the wrong length: it may truncate valid data or copy stale bytes. Fix by validating and using the incoming data's sof_abi_hdr.size from ucontrol before copying.	2026-08-15	7.8	CVE-2026-72304
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: fix VF bringup affecting PF promiscuous state Mbox handling of nix_set_rx_mode for a VF with promiscuous and all_multi flags set to false causes deletion of the PF's promiscuous and allmulti MCAM rules. This occurs because the APIs that	2026-08-15	7.9	CVE-2026-72312

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	enable/disable these rules operate only on the PF, even when the mbox request is made via a VF interface. Guard both rvu_npc_enable_allmulti_entry() and rvu_npc_enable_promisc_entry() disable paths with an is_vf() check so that a VF bringing up or tearing down its interface cannot inadvertently clear the PF's MCAM rules.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: regulator: core: regulator_lock_two() should test for EDEADLK not EDEADLOCK Compare against -EDEADLK, which is what ww_mutex_lock() actually returns and what every other deadlock check in this file already uses. Function regulator_lock_two() acquires two regulators via regulator_lock_nested() -> ww_mutex_lock(). On contention, ww_mutex_lock() returns -EDEADLK, which is the caller's signal to drop the lock it holds and retry the acquisition in the canonical order. However, regulator_lock_two() tests the return value against -EDEADLOCK rather than -EDEADLK. On most architectures, EDEADLK and EDEADLOCK are the same value, so the comparison happens to be correct and the bug is invisible. But on MIPS, SPARC, and PowerPC, those two errors have different values. The test is wrong: a genuine -EDEADLK backoff no longer matches -EDEADLOCK, so instead of unlocking and retrying, the code falls into WARN_ON(ret) and returns with only one of the two regulators locked. In practice, this is a bug only on MIPS, because the regulator core is not built or used on the other two platforms. In general, EDEADLK is preferred over EDEADLOCK for new code.	2026-08-15	7.8	CVE-2026-72314
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix busy dentry warning on unmount after DIO Commit c68337442f03 ("cifs: Fix busy dentry used after unmounting") fixed the issue in cifs where deferred close of a file led to a dentry reference count not being released in umount, by flushing deferredclose_wq in cifs_kill_sb() to solve it. However, the cifs DIO path suffers from the same busy-dentry problem caused by a delayed dentry reference-count release: [dio] [cifsd] [close + umount] netfs_unbuffered_write_iter_locked ... cifs_demultiplex_thread netfs_unbuffered_write cifs_issue_write netfs_wait_for_in_progress_stream [1] ... netfs_write_subrequest_terminated netfs_subreq_clear_in_progress netfs_wake_collector // wake [1] netfs_put_subrequest netfs_put_request queue_work(system_dfl_wq, xxx) [2] // dio write return cifs_close_cifsFileInfo_put // cfile->count 2->1 --cfile->count [3] // umount cifs_kill_sb kill_anon_super // warning triggered! shrink_dcache_for_umount [4] [system_dfl_wq] [5] netfs_free_request ... _cifsFileInfo_put // cfile->count 1->0 --cfile->count queue_work(fileinfo_put_wq, xxx) [fileinfo_put_wq] [6] cifsFileInfo_put_work cifsFileInfo_put_final dput If the umount path is triggered before [5], it results warning: BUG: Dentry 00000000eab1f070{i=9a917b66ae404fec,n=test} still in use (1) [umount of cifs cifs] The existing per-inode ictx->io_count wait in cifs_evict_inode() does not help: it lives in the inode eviction path, which runs after shrink_dcache_for_umount() has already warned about the busy dentries. Fix it by adding a per-superblock outstanding-rreq counter that is incremented in cifs_init_request() and decremented in cifs_free_request(). In cifs_kill_sb(), before kill_anon_super(), wait for this counter to reach 0 - which guarantees that all cleanup_work for this sb have run and thus all relevant cfile puts are queued on fileinfo_put_wq or serverclose_wq. Then drain the workqueue so the dentry refs are dropped. This is a targeted wait, not a flush of the system-wide system_dfl_wq.	2026-08-15	7.8	CVE-2026-72315
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix potential amdxdna_umap lifetime race amdxdna_umap_release() calls the blocking mmu_interval_notifier_remove() before removing the object from abo->mem.umap_list. If aie2_populate_range() runs concurrently, it may obtain a reference to an amdxdna_umap that is being released, leading to a potential use-after-free. Use kref_get_unless_zero() in aie2_populate_range() when acquiring a reference. If the reference count has already dropped to zero, release is in progress and the entry is skipped.	2026-08-15	7.8	CVE-2026-72328
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/tls: Consume empty data records in tls_sw_read_sock() A peer may send a zero-length TLS application_data record; TLS 1.3 explicitly permits these as a traffic-analysis countermeasure (RFC 8446, Section 5.1). After decryption such a record has full_len == 0. tls_sw_read_sock() hands it to the read_actor, which has no payload to consume and returns zero. The loop treats a zero return as backpressure (used <= 0), requeues the skb at the head of rx_list, and stops. rx_list is serviced head-first on the next call, so the empty record is dequeued, fails the same way, and is requeued again; every later record on the connection is blocked behind it.	2026-08-15	7.5	CVE-2026-72330

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	tls_sw_recvmg() does not stall on this: a zero-length data record copies nothing and falls through to consume_skb(). Mirror that in the read_sock() path by recognizing an empty data record before the actor runs, consuming it, and continuing.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix VMA access race aie2_populate_range() and amdxdna_umap_release() access a saved VMA pointer that may have already been freed, leading to a potential use-after-free. Remove the VMA accesses from these functions to avoid the race.	2026-08-15	7.8	CVE-2026-72331
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Fix adv monitor add failure cleanup hci_add_adv_monitor() publishes a new adv_monitor in hdev->adv_monitors_idr before the powered MSFT setup step. The MSFT offload add path can then fail either locally before the controller add command completes, or in the MSFT add callback. In the current queued management add flow, hci_cmd_sync_work() still invokes mgmt_add_adv_patterns_monitor_complete() with the original pending command after msft_add_monitor_pattern() returns. The buggy scenario involves two paths, with each column showing the order within that path: MSFT add handling MGMT completion 1. insert monitor and handle 1. receive sync error 2. send MSFT add command 2. call add-monitor completion 3. callback sees bad response 3. load cmd->user_data 4. callback frees monitor 4. read monitor->handle Local MSFT setup failures have the other half of the same ownership bug: they return an error after the IDR insertion, but no later code removes the failed monitor from the IDR. Keep ownership with the pending management command until its completion. For normal management adds, the MSFT add callback now records successful controller state and returns errors to its caller. The management completion frees the monitor on non-success after copying the response handle, while resume/reregister callback-error cleanup remains in the MSFT callback. The success path keeps the existing bookkeeping. Validation reproduced this kernel report: BUG: KASAN: slab-use-after-free in mgmt_add_adv_patterns_monitor_complete+0xfb/0x260 [bluetooth] Call Trace: <TASK> dump_stack_lvl+0x66/0xa0 print_report+0xce/0x5f0 ? mgmt_add_adv_patterns_monitor_complete+0xfb/0x260 [bluetooth] ? srso_alias_return_thunk+0x5/0xfbef5 ? __virt_addr_valid+0x19f/0x330 ? mgmt_add_adv_patterns_monitor_complete+0xfb/0x260 [bluetooth] kasan_report+0xe0/0x110 ? mgmt_add_adv_patterns_monitor_complete+0xfb/0x260 [bluetooth] mgmt_add_adv_patterns_monitor_complete+0xfb/0x260 [bluetooth] ? srso_alias_return_thunk+0x5/0xfbef5 ? 0xffffffffc00d00da ? __pfx_mgmt_add_adv_patterns_monitor_complete+0x10/0x10 [bluetooth] ? __pfx_mgmt_add_adv_patterns_monitor_complete+0x10/0x10 [bluetooth] ? hci_cmd_sync_work+0x1ab/0x210 [bluetooth] hci_cmd_sync_work+0x1c0/0x210 [bluetooth] ? __pfx_mgmt_add_adv_patterns_monitor_complete+0x10/0x10 [bluetooth] process_one_work+0x4fd/0xbc0 ? __pfx_process_one_work+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 ? srso_alias_return_thunk+0x5/0xfbef5 ? __list_add_valid_or_report+0x37/0xf0 ? __pfx_hci_cmd_sync_work+0x10/0x10 [bluetooth] ? srso_alias_return_thunk+0x5/0xfbef5 worker_thread+0x2d8/0x570 ? __pfx_worker_thread+0x10/0x10 kthread+0x1ad/0x1f0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x3c9/0x540 ? __pfx_ret_from_fork+0x10/0x10 ? srso_alias_return_thunk+0x5/0xfbef5 ? __switch_to+0x2e9/0x730 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> Allocated by task 471 on cpu 3 at 285.205389s: kasan_save_stack+0x33/0x60 kasan_save_track+0x17/0x60 __kasan_kmalloc+0xaa/0xb0 add_adv_patterns_monitor_rssi+0xd5/0x230 [bluetooth] hci_sock_sendmsg+0x96b/0xf80 [bluetooth] __sys_sendto+0x2bc/0x2d0 __x64_sys_sendto+0x76/0x90 do_syscall_64+0x115/0x6a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 454 on cpu 2 at 285.217112s: kasan_save_stack+0x33/0x60 kasan_save_track+0x17/0x60 kasan_save_free_info+0x3b/0x60 __kasan_slab_free+0x5f/0x80 kfree+0x313/0x590 msft_add_monitor_sync+0x54a/0x570 [bluetooth] hci_add_adv_monitor+0x133/0x180 [bluetooth] hci_cmd_sync_work+0x187/0x210 [bluetooth] process_one_work+0x4fd/0xbc0 worker_thread+0x2d8/0x570 kthread+0x1ad/0x1f0 ret_from_fork+0x3c9/0x540 ret_from_fork_asm+0x1a/0x30	2026-08-15	7.8	CVE-2026-72335

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_pedit: fix TOCTOU heap OOB write in tc offload There is a TOCTOU race condition in flower lockless approach between sizing a flow_rule buffer and filling it. zdi-disclosures@trendmicro.com reports: The cls_flower classifier operates with TCF_PROTO_OPS_DOIT_UNLOCKED (fl_change runs without RTNL), while RTM_NEWACTION holds RTNL, so the independent locking domains make the race reachable in practice. KASAN confirms: BUG: KASAN: slab-out-of-bounds in tcf_pedit_offload_act_setup+0x81b/0x930 Write of size 4 at addr ffff888001f27520 by task poc-toctou/312 The buggy address is located 0 bytes to the right of allocated 288-byte region [ffff888001f27400, ffff888001f27520) (cache kcalloc-512) Note: The result is a heap OOB write attacker-controlled content into the adjacent slab object (requires CAP_NET_ADMIN). The fix introduces reading tcfp_nkeys under act->tcfa_lock in all places using a new tcf_pedit_nkeys_locked() which replaces the old tcf_pedit_nkeys(). Additionally we close the remaining TOCTOU window between the sizing read and the fill reads by more careful accounting. Rather than silently truncating the key count, which leads to incorrect action semantics offloaded to hardware and secondary OOB writes if the remaining capacity is zero or consumed by prior actions, we enforce remaining capacity checks and return -ENOSPC if the required space exceeds the remaining capacity.	2026-08-15	7.8	CVE-2026-72338
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: microchip: vcap: fix races on the shared Super VCAP block The VCAP instances on a chip are not independent, yet they are locked independently. On sparx5 and lan969x the IS0 and IS2 instances are backed by the same Super VCAP hardware block and share its cache and command registers: every access drives the shared VCAP_SUPER_CTRL register and moves data through the shared cache registers. Accessing one instance therefore races with accessing another. The per-instance admin->lock cannot prevent this, as each instance takes a different lock. The locking issue is mostly disguised by the fact that the core usage of the vcap api runs under rtnl. However, the full rule dump in debugfs decodes rules straight from hardware (a READ command followed by a cache read) and runs outside rtnl, so it races a concurrent tc-flower rule write to another Super VCAP instance. Besides corrupting the dump, the read repopulates the shared cache between the writers cache fill and its write command, so the writer commits the wrong data and corrupts the hardware entry. Introduce vcap_lock() and vcap_unlock() helpers and route every rule lock site in the VCAP API and its debugfs code through them. Replace the per-instance admin->lock with a single mutex in struct vcap_control that serializes access to all instances. The helpers reach it through a new admin->vctrl back-pointer, and the clients initialise and destroy the control lock instead of a per-instance one. No path holds more than one instance lock, so collapsing them onto a single mutex cannot self-deadlock.	2026-08-15	7.8	CVE-2026-72340
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: TC, skip peer flow cleanup when LAG seq is unavailable mlx5_lag_get_dev_seq() will return error when the peer isn't in the LAG or when no device is marked as master. Result bad memory access and kernel crash[1]. Hence, skip the peer when lookup fails. Note: In case there are peer flows, they are cleaned before LAG cleared the master mark. [1] RIP: 0010:mlx5e_tc_del_fdb_peers_flow+0x3d/0x350 [mlx5_core] Call Trace: <TASK> mlx5e_tc_clean_fdb_peer_flows+0xc1/0x130 [mlx5_core] mlx5_esw_offloads_unpair+0x3a/0x400 [mlx5_core] mlx5_esw_offloads_devcom_event+0xee/0x360 [mlx5_core] mlx5_devcom_send_event+0x7a/0x140 [mlx5_core] mlx5_esw_offloads_devcom_cleanup+0x2f/0x90 [mlx5_core] mlx5e_tc_esw_cleanup+0x28/0xf0 [mlx5_core] mlx5e_rep_tc_cleanup+0x19/0x30 [mlx5_core] mlx5e_cleanup_uplink_rep_tx+0x36/0x40 [mlx5_core] mlx5e_cleanup_rep_tx+0x55/0x60 [mlx5_core] mlx5e_detach_netdev+0x96/0xf0 [mlx5_core] mlx5e_netdev_change_profile+0x5b/0x120 [mlx5_core] mlx5e_netdev_attach_nic_profile+0x1b/0x30 [mlx5_core] mlx5e_vport_rep_unload+0xdd/0x110 [mlx5_core] __esw_offloads_unload_rep+0x81/0xb0 [mlx5_core] mlx5e_eswitch_unregister_vport_reps+0x1d7/0x220 [mlx5_core] mlx5e_rep_remove+0x22/0x30 [mlx5_core] device_release_driver_internal+0x194/0x1f0 bus_remove_device+0xe8/0x1b0 device_del+0x159/0x3c0 mlx5_rescan_drivers_locked+0xbc/0x2d0 [mlx5_core] mlx5_unregister_device+0x54/0x80 [mlx5_core] mlx5_uninit_one+0x73/0x130 [mlx5_core] remove_one+0x78/0xe0 [mlx5_core] pci_device_remove+0x39/0xa0	2026-08-15	7.8	CVE-2026-72344

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: LAG, Fix off-by-one in single-FDB error rollback On failure at index i, the reverse cleanup loop in mlx5_lag_create_single_fdb() starts from i, so the failed index itself is rolled back. That can operate on uninitialized state or double-tear-down a rule the add_one path already self-rolled-back. Start the rollback from i - 1 so only successfully-installed entries are undone.	2026-08-15	7.8	CVE-2026-72345
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_connmark: reject invalid shift parameters Revision 2 of the CONNMARK target accepts user-controlled shift parameters and applies them to 32-bit mark values in connmark_tg_shift(). A shift_bits value of 32 or more triggers an undefined-shift bug when the rule is evaluated. Invalid shift_dir values are also accepted and silently fall back to the left-shift path. Reject invalid revision-2 shift parameters in connmark_tg_check() so malformed rules fail at installation time, before they can reach the packet path.	2026-08-15	7.3	CVE-2026-72347
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_u32: reject invalid shift counts u32_match_it() executes rule-supplied shift operands on a 32-bit value. A malformed u32 rule can provide a shift count of 32 or more, triggering an undefined shift out-of-bounds during packet evaluation. Validate XT_U32_LEFTSH and XT_U32_RIGHTSH operands in u32_mt_checkentry() and reject malformed rules before they reach the packet path.	2026-08-15	7.8	CVE-2026-72350
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: HID: bpf: Fix hid_bpf_get_data() range check hid_bpf_get_data() returns a pointer into the HID-BPF context data when the caller-provided offset and size fit inside ctx->allocated_size. The current check adds rdwr_buf_size and offset before comparing the result against ctx->allocated_size. Since both values are unsigned, a very large size can wrap the sum below ctx->allocated_size and make the helper return a pointer even though the requested range is not contained in the backing buffer. Use check_add_overflow() to reject wrapped range ends before comparing the requested range end against ctx->allocated_size.	2026-08-15	7.8	CVE-2026-72352
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: cifs: Fix missing credit release on failure in cifs_issue_read() Fix missing release of credits in the failure path in cifs_issue_read() lest retrying the subreq just overwrites the credits value.	2026-08-15	7.5	CVE-2026-72356
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: uprobes/x86: Use proper mm_struct in __in_uprobe_trampoline In the unregister path we use __in_uprobe_trampoline check with current->mm for the VMA lookup, which is wrong, because we are in the tracer context, not the traced process. Add mm_struct pointer argument to __in_uprobe_trampoline and changing related callers to pass proper mm_struct pointer.	2026-08-15	7.8	CVE-2026-72357
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/pt: prevent invalid cursor access for purged BOs During a page table walk for binding, xe_pt_stage_bind() explicitly skips initializing the xe_res_cursor for purged BOs, treating them similarly to NULL VMAs by only setting the cursor size. However, xe_pt_hugepte_possible() and xe_pt_scan_64K() did not check if the BO was purged before attempting to walk the cursor using xe_res_dma() and xe_res_next(). Because the cursor was left uninitialized for purged BOs, this falls through and triggers warnings like: WARNING: drivers/gpu/drm/xe/xe_res_cursor.h:274 at xe_res_next Fix this by explicitly checking if the BO is purged in both xe_pt_hugepte_possible() and xe_pt_scan_64K(), returning early just as we do for NULL VMAs, avoiding the invalid cursor accesses entirely. As a precaution, also zero-initialize the cursor in xe_pt_stage_bind() to ensure we don't pass garbage data into the page table walkers if we ever hit a similar edge case in the future. (cherry picked from commit 4c7b9c6ece32440e5a435a92076d049450cd2d2e)	2026-08-15	7.8	CVE-2026-72358
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfs: Fix writeback error handling Fix the error handling in writeback_iter() loop. If an error occurs, writeback_iter() needs to be called again with *error set to the error so that it can clean up iteration state. Further, the current folio needs unlocking and redirtying.	2026-08-15	7.1	CVE-2026-72364
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: cache/files: Fix double unlock in nomem_d_alloc error path When start_creating() fails and returns -ENOMEM, it has already released the parent directory lock in __start_dirop(): static struct dentry *__start_dirop(...) { ... inode_lock_nested(dir, I_MUTEX_PARENT); dentry = lookup_one_qstr_excl(name, parent, lookup_flags); if	2026-08-15	7.8	CVE-2026-72368

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(IS_ERR(dentry)) inode_unlock(dir); <-- Lock released on error return dentry; } However, the nomem_d_alloc error path in cachefiles_get_directory() unconditionally calls inode_unlock(d_inode(dir)) again, causing a double unlock that corrupts the rwsem state. This is a leftover from commit 7ab96df840e60 which replaced manual locking with start_creating() but failed to update the nomem_d_alloc path (while correctly updating mkdir_error and lookup_error paths).			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: minix: avoid overflow in bitmap block count calculation minix_check_superblock() uses minix_blocks_needed() to verify that the on-disk imap and zmap block counts are large enough for the advertised inode and zone counts. The helper currently performs DIV_ROUND_UP() in unsigned int arithmetic. A Minix v3 image can set s_ninodes or s_zones near UINT_MAX so the addition inside DIV_ROUND_UP() wraps to zero. That makes a zero imap/zmap block count look valid, after which minix_fill_super() can dereference s_imap[0] or s_zmap[0] even though no bitmap buffers were allocated. Impact: mounting a crafted Minix v3 image whose s_ninodes or s_zones is near UINT_MAX makes minix_check_superblock() accept a zero bitmap-block count and minix_fill_super() dereference s_imap[0]/s_zmap[0], panicking the kernel. The divisor is the bitmap capacity in bits, blocksize * 8, which is always a power of two: minix_fill_super() obtains the block size through sb_set_blocksize(), and blk_validate_block_size() rejects any size that is not a power of two. Use DIV_ROUND_UP_POW2(), which divides before adding the round-up term and so cannot overflow for a power-of-two divisor.	2026-08-15	7.8	CVE-2026-72369
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: Fix the volume AFS_VOLUME_RM_TREE is set on Fix afs_insert_volume_into_cell() to set AFS_VOLUME_RM_TREE on the volume replaced, not the new volume, as it's now removed from the cell's volume tree. This will cause the old volume to be removed from the tree twice and the new volume never to be removed.	2026-08-15	7.8	CVE-2026-72371
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: Fix lack of locking around modifications of net->cells_dyn_ino Fix the lack of locking around modifications of net->cells_dyn_ino by taking net->cells_lock exclusively. This also requires to cell to be removed from net->cells_dyn_ino in afs_destroy_cell_work() rather than in afs_cell_destroy() as the latter runs in RCU cleanup context and sleeping locks cannot be taken there.	2026-08-15	7.8	CVE-2026-72372
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: Fix missing NULL pointer check in afs_break_some_callbacks() Fix afs_break_some_callbacks() to check to see if afs_lookup_volume_rcu() returned NULL (e.g. the specified volume is unknown).	2026-08-15	7.5	CVE-2026-72373
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: Fix callback service message parsers to pass through -EAGAIN The AFS filesystem client uses an rxrpc server to listen for callback notifications. Each callback call type handler has a delivery function that parses the incoming request stream, and this should return -EAGAIN the last packet hasn't yet been seen, but all currently queued received data is consumed. afs_extract_data() does this, but the -EAGAIN return is switched to 0 inadvertently Fix callback service message parsers to pass through -EAGAIN	2026-08-15	7.5	CVE-2026-72374
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: Fix reinitialisation of the inode, in particular ->lock_work It seems that initialising afs_vnode::lock_work a single time in the slab's init function isn't sufficient for work_structs. This results in the DEBUG_OBJECTS debugging stuff producing a warning occasionally when running the generic/131 xfstest: ODEBUG: activate not available (active state 0) object: 0000000016d8760f object type: work_struct hint: afs_lock_work+0x0/0x220 WARNING: lib/debugobjects.c:629 at debug_print_object+0x4b/0x90, CPU#3: locktest/7695 ... CPU: 3 UID: 0 PID: 7695 Comm: locktest Tainted: G S 7.1.0-build3+ #2771 PREEMPT ... RIP: 0010:debug_print_object+0x65/0x90 ... Call Trace: <TASK> ? __pfx_afs_lock_work+0x10/0x10 debug_object_activate+0x122/0x170 insert_work+0x25/0x60 __queue_work+0x2e0/0x340 queue_delayed_work_on+0x48/0x70 afs_fl_release_private+0x57/0x70 locks_release_private+0x5c/0xa0 locks_free_lock+0xe/0x20 posix_lock_inode+0x55f/0x5b0 locks_lock_inode_wait+0x81/0x140 ? file_write_and_wait_range+0x50/0x70 afs_lock+0xcd/0x110 fcntl_setlk+0x10d/0x260 do_fcntl+0x24e/0x5b0 __do_sys_fcntl+0x6a/0x90 do_syscall_64+0x11e/0x310 entry_SYSCALL_64_after_hwframe+0x71/0x79 Fix this	2026-08-15	7.8	CVE-2026-72375

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by reinitialising ->lock_work after allocating an inode. Also, flush ->lock_work when the inode is being evicted to make sure it's not still running.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: Fix error code in afs_extract_vl_addrs() The error codes on these paths are only set on the first iteration through the loop. Set the correct error code on every iteration.	2026-08-15	7.5	CVE-2026-72378
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: fix addr_wq_timer race in sctp_free_addr_wq() sctp_free_addr_wq() previously removed addr_wq_timer using timer_delete() while holding addr_wq_lock. However, timer_delete() does not guarantee that a currently running timer handler has completed. This allows a race with sctp_addr_wq_timeout_handler(), where the handler may still run after addr_waitq has been freed, acquire addr_wq_lock, and access freed memory, leading to a use-after-free. Fix this by calling timer_shutdown_sync() before taking addr_wq_lock. This guarantees that any in-flight timer handler has finished and prevents the timer from being re-armed during teardown, making subsequent cleanup safe.	2026-08-15	7.8	CVE-2026-72383
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bridge: stp: Fix a potential use-after-free when deleting a bridge The three STP timers are not supposed to be armed while the bridge is administratively down. They are synchronously deactivated when the bridge is put administratively down and the various call sites check for 'IFF_UP' before arming them. This check is missing from br_topology_change_detection() and it is possible to engineer a situation in which the topology change timer is armed while the bridge is administratively down, resulting in a use-after-free [1] when the bridge is deleted. Fix by adding the missing check and for good measures synchronously shutdown the three timers when the bridge is deleted. [1] ODEBUG: free active (active state 0) object: ffff88811662b9b0 object type: timer_list hint: br_topology_change_timer_expired (net/bridge/br_stp_timer.c:120) WARNING: lib/debugobjects.c:629 at debug_print_object+0x1bc/0x450, CPU#9: ip/359	2026-08-15	7.8	CVE-2026-72389
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_teql: Introduce slaves_lock to avoid race condition and UAF The teql master->slaves singly linked list is not protected against multiple writes. It can be mod'ed concurrently from teql_master_xmit(), teql_dequeue(), teql_init() and teql_destroy() without holding any list lock or RCU protection. zdi-disclosures@trendmicro.com has demonstrated that the qdisc is freed after an RCU grace period, but teql_master_xmit() running on another CPU can still hold a stale pointer into the list, resulting in a slab-use-after-free: BUG: KASAN: slab-use-after-free in teql_master_xmit+0xf0f/0x16b0 Read of size 8 at addr ffff888013fb0440 by task poc/332 Freed 512-byte region [ffff888013fb0400, ffff888013fb0600] (kmalloc-512) The fix? Add a per-master slaves_lock spinlock that serializes all mutations of master->slaves and the NEXT_SLAVE() links in teql_destroy() and teql_qdisc_init(). teql_master_xmit() also takes the same slaves_lock around those updates. Annotate master->slaves and the per-slave ->next pointer with __rcu and use the appropriate RCU accessors everywhere they are touched: rcu_assign_pointer() on the writer side (under slaves_lock), rcu_dereference_protected() for the writer-side loads (also under slaves_lock), rcu_dereference_bh() for the loads in teql_master_xmit() and rtnl_dereference() for the loads in teql_master_open()/teql_master_mtu(), which run under RTNL. Pair this with rcu_read_lock_bh()/rcu_read_unlock_bh() around the list traversal in teql_master_xmit(), so that readers either observe a fully linked list or are deferred until the in-flight mutation completes. The two early-return paths in teql_master_xmit() are updated to release the RCU-bh read-side critical section before returning, since leaving it held would disable BH on that CPU for good.	2026-08-15	7.8	CVE-2026-72390
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (pmbus) Fix passing events to regulator core Sashiko reports: Commit 754bd2b4a084 ("hwmon: (pmbus/core) Protect regulator operations with mutex") introduced a worker to batch regulator events over time using atomic_or(). The delayed worker then passes the combined bitmask unmodified to regulator_notifier_call_chain(). The core regulator subsystem's regulator_handle_critical() function evaluates the event parameter using a strict switch statement. If multiple distinct faults occur before the worker runs (e.g., REGULATOR_EVENT_UNDER_VOLTAGE REGULATOR_EVENT_OVER_CURRENT), the combined bitmask fails to match any case. This leaves the reason as NULL and completely bypasses the critical hw_protection_trigger(). Fix the problem by passing events bit by bit to the regulator event handler.	2026-08-15	7.1	CVE-2026-72395

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (pmbus/core) honor vrm_version in pmbus_data2reg_vid() pmbus_data2reg_vid() hardcoded the VR11 encoding regardless of the vrm_version configured by the driver, while pmbus_reg2data_vid() already switched on it. Any driver that selects a non-VR11 VID mode and exposes a regulator (or hwmon vout setter) sent dangerously wrong codes to PMBUS_VOUT_COMMAND -- e.g. an nvidia195mv part asked for 200 mV got the VR11 clamp to 500 mV encoded as 0xB2, which the chip interprets as 1080 mV. Mirror pmbus_reg2data_vid() so writes round-trip with reads.	2026-08-15	7.1	CVE-2026-72397
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: seg6: validate SRH length before reading fixed fields seg6_validate_srh() reads fixed SRH fields such as srh->type and srh->hdrlen before checking that the supplied length covers the fixed struct ipv6_sr_hdr fields. The BPF SEG6 encap path reaches this with a BPF program-supplied pointer and length: bpf_lwt_push_encap() and the SEG6 local BPF END_B6 and END_B6_ENCAP actions call bpf_push_seg6_encap(), which forwards the length to seg6_validate_srh() with no minimum-size guard. A 2-byte SEG6 encap header can therefore make the validator read srh->type at offset 2 beyond the caller-supplied buffer. Reject lengths shorter than the fixed SRH at the top of seg6_validate_srh(), before any field is read. This fixes the BPF helper path and keeps the common validator robust.	2026-08-15	7.8	CVE-2026-72400
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: fix UAF in cleanup_bearer() due to premature dst_cache_destroy() TIPC UDP media bearer teardown calls dst_cache_destroy() on its replicast caches before calling synchronize_net() to wait for concurrent RCU readers (transmitters) to finish: static void cleanup_bearer(struct work_struct *work) { ... list_for_each_entry_safe(rcast, tmp, &ub->rcast.list, list) { dst_cache_destroy(&rcast->dst_cache); list_del_rcu(&rcast->list); kfree_rcu(rcast, rcu); } ... dst_cache_destroy(&ub->rcast.dst_cache); udp_tunnel_sock_release(ub->sk); synchronize_net(); ... } This is highly buggy because dst_cache_destroy() immediately frees the per-CPU cache memory (free_percpu()) and releases the cached dst entries without any synchronization. If a concurrent transmitter (e.g., tipc_udp_xmit()) is running on another CPU under RCU protection, it can call dst_cache_get() concurrently, leading to: 1. Use-After-Free on the per-CPU cache pointer itself (crash). 2. "rcuref - imbalanced put()" warning if it attempts to release a dst that was concurrently released by dst_cache_destroy(). Furthermore, calling kfree(ub) immediately after synchronize_net() without closing the socket first (or waiting after closing it) leaves a window where a concurrent receiver (tipc_udp_rcv()) could start after synchronize_net(), access ub, and suffer a UAF when kfree(ub) runs. To fix this, we must defer dst_cache_destroy() and kfree(ub) until after we have ensured that no more readers can see the bearer/socket and all existing readers have finished: 1. Defer rcast entry destruction (both dst_cache_destroy() and kfree()) to an RCU callback using call_rcu_hurry(). Using call_rcu_hurry() ensures the dst entries are released quickly. 2. Release the bearer socket using udp_tunnel_sock_release() (stops new receive readers). 3. Call synchronize_net() to wait for all outstanding RCU readers (both transmit and receive) to finish. 4. Now that it is safe, call dst_cache_destroy() on the main bearer cache, and free ub. Note: 3) and 4) can be changed later in net-next to also use call_rcu_hurry() and get rid of the synchronize_net() latency.	2026-08-15	7.8	CVE-2026-72404
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: udp_tunnel: prevent double queueing in udp_tunnel_nic_device_sync Yue Sun reported a use-after-free and debugobjects warning in udp_tunnel_nic_device_sync_work() during concurrent device operations. The workqueue core clears the internal pending bit before invoking the worker. At that point, a concurrent thread can queue the work again. When the already running worker eventually clears the work_pending flag to 0, it mistakenly clears the flag for the newly queued instance. udp_tunnel_nic_unregister() then observes work_pending as 0 and frees the structure while the second work item is still active in the queue, leading to UAF. Fix this by returning early in udp_tunnel_nic_device_sync() if work_pending is already set, preventing redundant work queueing.	2026-08-15	7.8	CVE-2026-72405
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: sungem: fix probe error cleanup gem_init_one() calls gem_remove_one() when register_netdev() fails. gem_remove_one() unregisters and frees resources owned by the net_device, including the DMA block, MMIO mapping, PCI regions, and the net_device itself. gem_init_one() then falls through to its own cleanup labels and frees the same resources again. Keep the register_netdev() error path in	2026-08-15	7.8	CVE-2026-72406

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	gem_init_one(): clear drvdata so PM/remove paths do not see a half-registered device, remove the NAPI instance added during probe, and let the existing cleanup labels release the resources once. The issue was found by a local static-analysis checker for probe error paths. The reported path was manually inspected before sending this fix. Compile-tested with CONFIG_SUNGEM=y. Runtime testing was not performed because no sungem hardware is available.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mvneta: re-enable percpu interrupt on resume On Marvell MPIC platforms (Armada 370/XP/38x), mvneta uses a percpu IRQ disable/enable scheme for NAPI: the ISR (mvneta_percpu_isr) calls disable_percpu_irq() to mask the MPIC per-CPU interrupt and schedules NAPI poll, which calls enable_percpu_irq() on completion to unmask. If suspend occurs while NAPI poll is pending (between disable_percpu_irq in the ISR and enable_percpu_irq in poll completion), the interrupt is never re-enabled: 1. mvneta_percpu_isr: disable_percpu_irq() + napi_schedule() => MPIC masked, percpu_enabled cpumask bit cleared 2. NAPI poll does not complete before suspend proceeds (on PREEMPT_RT this is highly likely since softirqs run in ksoftirqd which gets frozen; on non-RT it can happen when softirq processing is deferred to ksoftirqd) 3. mvneta_stop_dev => napi_disable(): cancels the pending poll without executing the completion path 4. suspend_device_irqs => IRQCHIP_MASK_ON_SUSPEND: masks MPIC (already masked, but records IRQS_SUSPENDED) 5. Resume: mpic_resume checks irq_percpu_is_enabled() => false (bit was cleared in step 1) => skips unmask 6. mvneta_start_dev only restores device-level INTR_NEW_MASK, does not touch the MPIC per-CPU mask Result: MPIC per-CPU interrupt stays masked permanently. The NIC generates interrupts (INTR_NEW_CAUSE != 0) but the CPU never receives them, causing complete loss of network connectivity. Fix by calling on_each_cpu(mvneta_percpu_enable) in the resume path to unconditionally unmask the MPIC per-CPU interrupt regardless of pre-suspend state.	2026-08-15	7.5	CVE-2026-72409
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: Validate NIX maximum LFs correctly NIX maximum number of LFs can be set via devlink command but that can be done before assigning any LFs to a PF/VF. The condition used to check whether any LFs are assigned is incorrect. This patch fixes that condition.	2026-08-15	7.8	CVE-2026-72410
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mxl862xx: fix use-after-free of DSA ports in crc_err_work Upon an MDIO CRC error mxl862xx_crc_err_work_fn() walks the DSA ports and closes the CPU port conduits: dsa_switch_for_each_cpu_port(dp, priv->ds) dev_close(dp->conduit); mxl862xx_remove() unregisters the switch before cancelling this work: set_bit(MXL862XX_FLAG_WORK_STOPPED, &priv->flags); cancel_delayed_work_sync(&priv->stats_work); dsa_unregister_switch(ds); mxl862xx_host_shutdown(priv); dsa_unregister_switch() frees the dsa_port objects. If a CRC error schedules the work during teardown it can run after the ports have been freed and dereference freed memory. Guard the port walk with MXL862XX_FLAG_WORK_STOPPED, which is already set before dsa_unregister_switch(). DSA tears the ports down under rtnl_lock(), so checking the flag under rtnl_lock() means the work either runs before teardown and sees valid ports, or runs afterwards, observes the flag and skips the walk. This mirrors the host_flood_work handler, which skips torn-down ports under rtnl_lock().	2026-08-15	7.8	CVE-2026-72411
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SDCA: Validate written enum value in ge_put_enum_double() ge_put_enum_double() passes the user-supplied enumeration index item[0] to snd_soc_enum_item_to_val() without checking it against the number of items in the enum: ret = snd_soc_enum_item_to_val(e, item[0]); snd_soc_enum_item_to_val() indexes the heap-allocated e->values[] array with that index (e->values is set from a devm_kcalloc() of e->items entries), so a control write with an out-of-range item[0] reads past the end of the values buffer. The bounds check in snd_soc_dapm_put_enum_double() only runs afterwards, so it does not prevent the read here. Reject an out-of-range item before using it, matching the other enum put handlers. This issue was pointed out by the Sashiko AI review bot while reviewing a related enum-validation series: https://lore.kernel.org/all/20260609125735.CEB651F00893@smtp.kernel.org/	2026-08-15	7.1	CVE-2026-72415
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_compat: ebttables emulation must reject non-bridge targets xtables targets return netfilter verdicts: NF_ACCEPT, NF_DROP, and so on. ebttables targets return incompatible verdicts: EBT_ACCEPT, EBT_DROP, ... We cannot allow fallback to	2026-08-15	7.3	CVE-2026-72416

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	NFPROTO_UNSPEC. ebttables doesn't permit this since 11ff7288beb2 ("netfilter: ebttables: reject non-bridge targets") but that commit missed the nft_compat layer.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conncount: prevent connlimit drops for early confirmed ct Commit 69894e5b4c5e ("netfilter: nft_connlmit: update the count if add was skipped") introduced a regression where packets for valid connections are dropped when using connlimit for soft-limiting scenarios. The issue occurs when a new connection reuses a socket currently in the TIME_WAIT state. In this scenario, the connection tracking entry is evaluated as already confirmed. Previously, __nf_conncount_add() assumed that if a connection was confirmed and did not originate from the loopback interface, it should skip the addition and return -EEXIST. Skipping the addition triggers a garbage collection run that cleans up the TIME_WAIT connection. Consequently, the active connection count drops to 0, which xt_connlmit mishandles, leading to the false rejection of the perfectly valid new connection. Fix this by replacing the interface check with protocol-agnostic state checks. We now skip the tree insertion and preserve the lockless garbage collection optimization only if the connection is IPS_ASSURED. This allows early-confirmed setup packets (such as reused TIME_WAIT sockets or locally generated SYN-ACKs) to be properly evaluated and counted without falsely dropping. The goto check_connections path is maintained to ensure these setup packets are deduplicated correctly. This has been tested with slowhttptest and HTTP server configured locally to ensure we are not breaking soft-limiting scenarios for local or external connections. In addition, it was tested with a OVS zone limit too.	2026-08-15	7.5	CVE-2026-72418
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_nat: avoid invalid nat_net pointer use on failed nf_nat_init() We ran into below KASAN splat, which is mostly uninteresting, beside for having nf_nat_register_fn() in the call chain as a cause for the offending access: ===== BUG: KASAN: slab-out-of-bounds in nf_nat_register_fn+0x5f9/0x640 Read of size 8 at addr ffff890031e54c20 by task iptables/9510 CPU: 0 UID: 0 PID: 9510 Comm: iptables Not tainted 6.18.18-grsec-full-20260320181326 #1 PREEMPT(voluntary) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: ffff88004117f8b0] ? ffff88004117fbc8 entry_SYSCALL_64_safe_stack+0x4a/0x60 ffff88004117fef8 </TASK> ===== The out-of-bounds report, though, is a red herring as it is f---truncated---	2026-08-15	7.8	CVE-2026-72419
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ice: fix FDIR CTRL VSI resource leak in ice_reset_all_vfs() Resetting all VFs causes resource leak on VFs with FDIR filters enabled as CTRL VSIs are only invalidated and not freed. Fix by using ice_vf_ctrl_vsi_release() instead of ice_vf_ctrl_invalidate_vsi() which aligns behavior with the ice_reset_vf() function. Reproduction: echo 1 > /sys/class/net/\$pf/device/sriov_numvfs ethtool -N \$vf flow-type ether proto 0x9000 action 0 echo 1 > /sys/class/net/\$pf/device/reset	2026-08-15	7.1	CVE-2026-72425
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix effective prog array index with BPF_F_PREORDER replace_effective_prog() and purge_effective_progs() located the slot in the effective array by walking the program hlist and counting entries linearly. That count does not match the array layout: compute_effective_progs() places BPF_F_PREORDER programs at the front (ancestor cgroup first, attach order within a cgroup) and the rest after them (descendant cgroup first). So when a preorder program is present, the linear hlist position no longer equals the program's index in the effective array. For replace_effective_prog() (bpf_link_update()) this overwrote the wrong slot, corrupting the effective order. For purge_effective_progs(), it could dummy out a slot belonging to a different program and leave the detached program in the array while bpf_prog_put() drops its reference, i.e. a use-after-free. Fix both by replaying compute_effective_progs()'s placement (including the per-cgroup preorder reversal) in a shared effective_prog_pos() helper. Identify the entry by its struct bpf_prog_list pointer rather than by (prog, link) value, so the lookup resolves to exactly the attachment the syscall selected even when the same bpf_prog is attached to several cgroups in the hierarchy.	2026-08-15	7.8	CVE-2026-72427
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: make sure gc is properly stopped Sashiko noticed that when destroying a set, cancel_delayed_work_sync() was called while gc calls queue_delayed_work() unconditionally which can lead not to properly shutting down the gc.	2026-08-15	7.8	CVE-2026-72434

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix order of kfree_rcu() and rcu_assign_pointer() Sashiko pointed out that kfree_rcu() was called before rcu_assign_pointer() in handling the comment extension. Fix the order so that rcu_assign_pointer() called first.	2026-08-15	7.8	CVE-2026-72435
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: md/raid10: fix writes_pending and barrier reference leaks on discard failures raid10_make_request() acquires a writes_pending reference with md_write_start() before calling raid10_handle_discard(). Several failure paths in raid10_handle_discard() complete the bio and return without releasing the corresponding reference, causing md_write_end() to be skipped. Call md_write_end() before returning from these failure paths to keep writes_pending accounting balanced. Additionally, discard split allocation failures can occur after wait_barrier() succeeds. Those paths return without calling allow_barrier(), leaking the associated barrier reference. Release the barrier before returning from those paths.	2026-08-15	7.5	CVE-2026-72438
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: md/raid1: fix writes_pending and barrier reference leaks on write failures raid1_make_request() acquires a writes_pending reference with md_write_start() before calling raid1_write_request(). Several failure paths in raid1_write_request() complete the bio and return without reaching the normal write completion path, causing the corresponding md_write_end() to be skipped. Make raid1_write_request() return a status indicating whether the write request was successfully queued. This allows raid1_make_request() to call md_write_end() when raid1_write_request() fails. Additionally, if wait_blocked_rdev() fails after wait_barrier() succeeds, the associated barrier reference is not released. Call allow_barrier() before returning from that path to keep the barrier accounting balanced.	2026-08-15	7.1	CVE-2026-72440
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: flow_dissector: check device type before reading ETH_ADDRS __skb_flow_dissect() unconditionally reads 12 bytes from eth_hdr(skb) when FLOW_DISSECTOR_KEY_ETH_ADDRS is requested. This assumes the skb has a valid Ethernet header at mac_header, which is not always the case. The problem can be triggered by: 1. Creating a TUN device in L3 mode (IFF_TUN, hard_header_len=0) 2. Attaching a multiq qdisc with a flower filter matching on eth_src 3. Sending a packet through AF_PACKET Since TUN in L3 mode has no link-layer header, mac_header points to the L3 data area. The flow dissector reads 12 bytes of uninitialized skb memory, which then propagates through fl_set_masked_key() and is used as a rhashtable lookup key in __fl_lookup(), as reported by KMSAN. Rejecting the filter in the control path (at tc filter add time) is not feasible because TC filter blocks can be shared between arbitrary devices -- a filter installed on an Ethernet device may later classify packets on a headerless device through a shared block. The device association is not fixed at filter creation time. Fix this by gating the memcpy on dev->type == ARPHRD_ETHER, which ensures only true Ethernet-framed packets have their addresses read. This is more precise than the previous hard_header_len >= 12 check, which would incorrectly pass for non-Ethernet link types like IPoB (ARPHRD_INFINIBAND, hard_header_len=24) and FDDI (hard_header_len=21) whose L2 headers are not in Ethernet format. Additionally check skb_mac_header_was_set() to guard against the pathological case where mac_header is the unset sentinel (~0U), which would cause eth_hdr() to return a wild pointer. For the act_mirred redirect case (Ethernet packet redirected to a non-Ethernet device sharing a TC block), zeroing the key is the correct behavior: the packet is now being classified on the target device, where Ethernet address matching is not semantically meaningful. Note: on non-Ethernet devices, the zeroed key will match a filter configured with all-zero MAC addresses. This is an improvement over the previous behavior where uninitialized memory could randomly match any filter.	2026-08-15	7.8	CVE-2026-72444
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: qcom: reject stream disable with no active interface handle_uaudio_stream_req() resolves an interface index with info_idx_from_ifnum(), which returns -EINVAL when no interface matches. The enable branch and the response: cleanup label both guard against a negative index, but the disable branch does not: it forms info = &uadev[pcm_card_num].info[info_idx] and dereferences it. uadev[] is a pointer allocated only when a stream is first enabled, so a negative info_idx on the disable path is unsafe in two ways: - If the card was never enabled, .info is NULL and &info[-EINVAL] is a wild pointer; reading info->data_ep_pipe faults (kernel oops). - If the card was enabled at least once (.info allocated) and the disable	2026-08-15	7.8	CVE-2026-72446

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	names an interface that does not match, &info[-EINVAL] points before the allocation; info->data_ep_pipe / info->sync_ep_pipe are an out-of-bounds slab read and, when non-zero, an out-of-bounds 4-byte write (both pipe fields are cleared to 0). That is memory corruption, not just a NULL dereference. The request is reachable from unprivileged local userspace over AF_QIPCRTR. Reject a disable request with no resolved interface, matching the guard the enable path already has.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: fix list_del corruption in kfd_criu_resume_svm The cleanup tail of kfd_criu_resume_svm() walks svms->criu_svm_metadata_list and kfree()s each struct criu_svm_metadata without removing it from the list. The list head is left pointing at freed kmalloc-96 objects. A second AMDKFD_IOC_CRIU_OP from the same process re-enters: list_empty() reads the dangling ->next (use-after-free), the loop walks freed entries, and each is kfree()d again (double-free). This is reachable by an unprivileged render-group user via /dev/kfd with no capabilities required. Add list_del() before the kfree() so the list is properly emptied. The list_for_each_entry_safe() iterator already caches the next pointer, so unlinking during the walk is safe. (cherry picked from commit 6322d278a298e2c1430b9d2697743d3a04b788b1)	2026-08-15	7.8	CVE-2026-72449
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: validate selector family and prefixlen during match syzbot reported a shift-out-of-bounds in xfrm_selector_match() due to AF_UNSPEC selector with large prefixlen (e.g. 128) matched against IPv4 flow (when XFRM_STATE_AF_UNSPEC is set). Fix this by: - Rejecting mismatched families in xfrm_selector_match. - Returning false in addr4_match if prefixlen > 32. - Returning false in addr_match if prefixlen > 128 (prevents overflow).	2026-08-15	7.8	CVE-2026-72450
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/i915: clear CRTC color blob pointers after dropping refs intel_crtc_put_color_blobs() drops the CRTC color blob references, but leaves the corresponding pointers unchanged. This can matter in intel_crtc_prepare_cleared_state(), which frees the old CRTC hw state before calling intel_dp_tunnel_atomic_clear_stream_bw(). The latter can fail while looking up the DP tunnel group state, for example with -EDEADLK. If that happens, the function returns without completing the cleared state preparation. The failed atomic state will then be cleared by the atomic core and intel_crtc_free_hw_state() can be called again for the same state, dropping the same blob references again. Clear the blob pointers after dropping the references so repeated cleanup of the same CRTC hw state is safe. (cherry picked from commit d5005addb5f68e8a0edce249506757bdc9e3d8c8)	2026-08-15	7.8	CVE-2026-72452
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: i3c: mipi-i3c-hci: Fix race in i3c_hci_addr_to_dev() i3c_hci_addr_to_dev() walks bus->devs.i3c, which is protected by bus.lock (rwsem). However, it is invoked from the MIPI I3C HCI IRQ handler, which cannot take bus.lock. This allows concurrent device addition/removal in the I3C core to modify the list while it is being traversed, potentially leading to use-after-free or crashes. Remove the dependency on the bus device list and introduce a dedicated lookup table. Add an ibi_devs[] array indexed by DAT entry, maintained under hci->lock. Update the array when IBIs are enabled or disabled, so that it always reflects the set of devices allowed to generate IBIs. Also update when IBIs are freed, to cover the corner case when an IBI is freed without first being disabled (e.g. olddev in i3c_master_add_i3c_dev_locked()). Move i3c_hci_addr_to_dev() into core.c, reimplement it using the new array, and add a lockdep assertion to enforce that hci->lock is held by callers. Demote a message in PIO and DMA IBI handling, from an error to a debug message, because there is a race window when the condition can arise normally.	2026-08-15	7.8	CVE-2026-72454
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix uninitialised pointer passed to audit_log_untrustedstring() Commit 4a134723f9f1 ("apparmor: move check for aa_null file to cover all cases") introduced a small bug, where path_name() may pass a potentially uninitialized *name to aa_audit_file() if the path->dentry had been replaced with aa_null.dentry earlier on. This can lead to page fault like one observed on 7.0.2 openSUSE Tumbleweed kernel: [51692.242756] [T24690] BUG: unable to handle page fault for address: 00000000f00000003 [51692.242762] [T24690] #PF: supervisor read access in kernel mode [51692.242763] [T24690] #PF: error_code(0x0000) - not-present page [51692.242765] [T24690] PGD 0 P4D 0 [51692.242768] [T24690] Oops: Oops: 0000 [#1] SMP NOPTI [51692.242772] [T24690] CPU: 3 UID: 1020 PID: 24690	2026-08-15	7.1	CVE-2026-72455

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Comm: snap-confine Tainted: G O 7.0.2-1-default #1 PREEMPT(full) openSUSE Tumbleweed ab90b4c9940707f9cafa19bdad80b2cec52dbe51 [51692.242775] [T24690] Tainted: [O]=OOT_MODULE [51692.242777] [T24690] Hardware name: Framework Laptop 13 (AMD Ryzen 7040Series)/FRANMDCP05, BIOS 03.18 01/08/2026 [51692.242778] [T24690] RIP: 0010:strlen+0x4/0x30 [51692.242783] [T24690] Code: f7 75 ec 31 c0 e9 17 9f 00 ff 48 89 f8 e9 0f 9f 00 ff 0f 1f 40 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa <80> 3f 00 74 18 48 89 f8 0f 1f 40 00 48 83 c0 01 80 38 00 75 f7 48 [51692.242785] [T24690] RSP: 0018:ffffd015eb1e3608 EFLAGS: 00010282 [51692.242787] [T24690] RAX: 0000000000000000 RBX: ffff89796198a360 RCX: 0000000000000000 [51692.242788] [T24690] RDX: 00000000000000d1 RSI: 0000000f00000003 RDI: 0000000f00000003 [51692.242790] [T24690] RBP: ffffffff7ede090 R08: 000000000000005f R09: 0000000000000000 [51692.242791] [T24690] R10: 0000000000000000 R11: 0000000000000000 R12: fffffd015eb1e3700 [51692.242792] [T24690] R13: ffff8977a22bc380 R14: ffffffff7ec5190 R15: ffff8977a0c8aa80 [51692.242794] [T24690] FS: 0000000000000000(0000) GS:ffff897f640d8000(0000) knlGS:0000000000000000 [51692.242796] [T24690] CS: 0010 DS: 0000 ES: 0000 CRO: 0000000080050033 [51692.242797] [T24690] CR2: 0000000f00000003 CR3: 00000006ad15f000 CR4: 0000000000f50ef0 [51692.242799] [T24690] PKRU: 55555554 [51692.242800] [T24690] Call Trace: [51692.242802] [T24690] <TASK> [51692.242804] [T24690] audit_log_untrustedstring+0x1d/0x40 [51692.242811] [T24690] common_lsm_audit+0x71/0x1d0 [51692.242816] [T24690] aa_audit+0x5a/0x170 [51692.242819] [T24690] aa_audit_file+0x18a/0x1b0 [51692.242825] [T24690] path_name+0xd2/0x100 [51692.242829] [T24690] profile_path_perm.part.0+0x58/0xb0 [51692.242832] [T24690] aa_path_perm+0xef/0x150 [51692.242837] [T24690] apparmor_file_open+0x153/0x2e0 [51692.242840] [T24690] security_file_open+0x46/0xd0 [51692.242844] [T24690] do_dentry_open+0xe9/0x4d0 [51692.242848] [T24690] vfs_open+0x30/0x100 While here, initialise variables which are passed down to path_name().			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: aa_label_alloc use aa_label_free on alloc failure aa_label_alloc() allocates a secid before allocating or taking the label proxy. If the later proxy step fails, the error path only freed the label memory, leaking any resources initialized by aa_label_init(). Use aa_label_free() on the failure path so partially initialized labels release their secid and other label resources before the backing memory is freed.	2026-08-15	7.8	CVE-2026-72459
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: check label build before no_new_privs test aa_change_profile() builds a replacement label with fn_label_build_in_scope() before the no_new_privs subset check. The build helper can fail and return NULL or an ERR_PTR, but the result was passed to aa_label_is_unconfined_subset() before the existing IS_ERR_OR_NULL() check. Reuse the existing target-label build failure handling immediately after the build. This preserves the current audit handling while preventing the subset helper from dereferencing an invalid label.	2026-08-15	7.1	CVE-2026-72460
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix refcount leak when updating the sk_ctx Currently update_sk_ctx() transfers the plabel reference, unfortunately it is also unconditionally put in the caller. Ideally we would make the caller conditionally put the reference based on whether it was transferred but for now just fix the bug by getting a reference.	2026-08-15	7.8	CVE-2026-72461
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xprtrdma: Repost Receive buffers for malformed replies rprcrdma_wc_receive() decrements the transport's Receive count for every completion before it dispatches a successful Receive to rprcrdma_reply_handler(). The handler must post a replacement Receive WR before returning unless ownership of the rep has moved elsewhere, as on the backchannel path. Commit 2ae50ad68cd7 ("xprtrdma: Close window between waking RPC senders and posting Receives") moved the Receive refill out of rprcrdma_wc_receive(), where it had run ahead of every reply, into rprcrdma_reply_handler() so that the responder's credit grant could be parsed before reposting. The bad-version and short-reply exits never reach that refill: they recycle the rep and return without calling rprcrdma_post_recvs(). A remote peer can therefore drain the client's posted Receive queue by sending a sustained stream of replies that are shorter than the fixed transport header or that carry an unrecognized RPC/RDMA version. Each such reply consumes one posted Receive without replacing it. Once the queue empties, the peer's next Send finds no posted	2026-08-15	7.5	CVE-2026-72464

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Receive and the transport stalls until reconnect. Route both malformed-reply exits through the shared repost tail after recycling the rep, refilling against buf->rb_credits, the most recent accepted credit grant. Neither exit updates the congestion window, so RPCs admitted under the previous grant remain in flight awaiting replies. A smaller refill target would let a stream of malformed replies ratchet the posted Receive count down to the batch floor while the congestion window still admits rb_credits RPCs; a burst of valid replies to those RPCs could then overrun the posted Receives, and because the client connects with rnr_retry_count of zero, a single RNR NAK terminates the connection. Refilling against rb_credits also restores the target that applied to malformed replies before commit 2ae50ad68cd7 ("xprtrdma: Close window between waking RPC senders and posting Receives") when rprcdma_post_recvs() computed it from rb_credits internally. rb_credits is at least one from connection establishment onward, so the repost path always keeps Receives posted.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xprtrdma: Sanitize the reply credit grant after parsing The out_norqst exit in rprcdma_reply_handler() branches away before the credit clamp, so a reply that matches no pending request reaches out_post carrying the raw credit value parsed from the wire. rprcdma_post_recvs() does not bound its @needed argument: the refill loop allocates and chains Receive WRs until the count is satisfied or allocation fails. A peer that sends a well-formed reply carrying an unknown XID and an inflated credit grant therefore drives rep allocation and Receive posting past re_max_requests on every such reply. Move the clamp to immediately after the credit field is parsed, ahead of the first branch that can reach out_post, so every later consumer sees a sanitized value. The cwnd update stays on the matched-request path.	2026-08-15	7.5	CVE-2026-72465
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: resize log->one_page_buf when adopting on-disk page size log_replay() allocates log->one_page_buf using the page size that was chosen from the host PAGE_SIZE: log->one_page_buf = kmalloc(log->page_size, GFP_NOFS); Later, when a restart area is found, the log page size recorded on disk is adopted: t32 = le32_to_cpu(log->rst_info.r_page->sys_page_size); if (log->page_size != t32) { log->l_size = log->orig_file_size; log->page_size = norm_file_page(t32, &log->l_size, t32 == DefaultLogPageSize); } If the on-disk page size is larger than the size used for the initial allocation, log->page_size grows but one_page_buf is left at its original, smaller size. A subsequent unaligned read_log_page() then reads log->page_size bytes into the undersized scratch buffer: page_buf = page_off ? log->one_page_buf : *buffer; err = ntfs_read_run_nb_ra(ni->mi.sbi, &ni->file.run, page_vbo, page_buf, log->page_size, NULL, &log->read_ahead); overflowing the allocation. This is reachable when mounting a dirty NTFS volume whose log was formatted with a page size larger than the buffer initially allocated on the mounting host (for example a 64K-log volume mounted on a host that allocated a 4K scratch buffer). Grow one_page_buf when the adopted on-disk page size exceeds the size used for the initial allocation. On krealloc() failure the original buffer is left intact and freed by the existing error path.	2026-08-15	7.8	CVE-2026-72470
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: prevent potential lcn remains uninitialized The target VCN being sought was not found within runs[0], causing run_lookup() to return false. This causes run_lookup_entry() to return false, which in turn results in a len value of 0, and the new parameter passed to attr_data_get_block() is NULL. Collectively, these factors ultimately cause attr_data_get_block_locked() to exit prematurely without initializing lcn, thereby triggering [1]. To prevent [1], the clen check within ni_seek_data_or_hole() has been moved to occur before the lcn check. [1] BUG: KMSAN: uninit-value in ni_seek_data_or_hole+0x24f/0x5f0 fs/ntfs3/frecord.c:2862 ni_seek_data_or_hole+0x24f/0x5f0 fs/ntfs3/frecord.c:2862 ntfs_llseek+0x22a/0x4a0 fs/ntfs3/file.c:1530 vfs_llseek fs/read_write.c:391 [inline]	2026-08-15	7.1	CVE-2026-72471
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dmaengine: Fix possible use after free In dma_release_channel(), check chan->device->privatcnt after call dma_chan_put(). However, dma_chan_put() call dma_device_put() which could release the last reference of the device if the DMA provider is already gone and hence free it. Fixes it by moving dma_chan_put() after the check.	2026-08-15	7.8	CVE-2026-72476
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iio: adc: xilinx-ams: fix out-of-bounds channel lookup in event handling ams_event_to_channel() may return a pointer past the end of dev->channels when no matching scan_index is found. This can lead to invalid memory access in ams_handle_event(). Add a	2026-08-15	7.8	CVE-2026-72480

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bounds check in <code>ams_event_to_channel()</code> and return NULL when no channel is found. Also guard the caller to safely handle this case.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gpib: fix double decrement of <code>descriptor_busy</code> in <code>command_ioctl()</code> commit d1857f8296dc ("gpib: fix use-after-free in IO ioctl handlers") introduced a <code>descriptor_busy</code> reference counter to pin struct <code>gpib_descriptor</code> across IO ioctl operations. In <code>command_ioctl()</code> , the error path inside the loop decrements <code>descriptor_busy</code> and breaks, but execution then falls through to the unconditional decrement after the loop, underflowing the counter to -1. This re-enables the use-after-free that the original fix was meant to prevent: a concurrent <code>close_dev_ioctl()</code> sees <code>descriptor_busy == 0</code> on an actively-used descriptor and frees it. Remove the early decrement from the error path. The post-loop decrement already handles all exit paths, matching the correct pattern used in <code>read_ioctl()</code> and <code>write_ioctl()</code> .	2026-08-15	7.8	CVE-2026-72482
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: usb: host: max3421: Fix shift-out-of-bounds in <code>max3421_hub_control()</code> The <code>'max3421_hub_control()'</code> function handles USB hub class requests to the virtual root hub. In the <code>'default'</code> branches of both the <code>'ClearPortFeature'</code> and <code>'SetPortFeature'</code> switch statements, it modifies <code>'max3421_hcd->port_status'</code> by left shifting 1 by the request's <code>'value'</code> parameter. However, it does not validate whether this shift will exceed the width of <code>'port_status'</code> . So if a malicious userspace task with access to the root hub via <code>/dev/bus/usb/.../001</code> issues a <code>USBDEVFS_CONTROL</code> ioctl with <code>'wValue'</code> greater than or equal to 32, the left shift operation invokes shift-out-of-bounds undefined behavior. This results in arbitrary bit corruption of <code>'port_status'</code> , including the normally-immutable change bits, which can bypass internal state checks and confuse the hub status. Fix this by rejecting requests whose <code>'value'</code> exceeds the shift width before performing the shift. This issue was found using a KLEE-based symbolic execution tool for kernel drivers that I'm currently developing.	2026-08-15	7.8	CVE-2026-72483
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: coresight: platform: defer connection counter increment until alloc succeeds <code>coresight_add_out_conn()</code> increments <code>nr_outconns</code> before calling <code>devm_krealloc_array()</code> and again before <code>devm_kmalloc()</code> . If either allocation fails, the counter is already bumped while the corresponding array entry is NULL or uninitialized garbage. <code>coresight_add_in_conn()</code> has the same problem with <code>nr_inconns</code> and <code>devm_krealloc_array()</code> . In both cases the probe returns <code>-ENOMEM</code> , which causes <code>coresight_get_platform_data()</code> to call <code>coresight_release_platform_data()</code> for cleanup. That function iterates up to <code>nr_outconns</code> (or <code>nr_inconns</code>) entries and dereferences each pointer unconditionally, hitting the NULL or garbage entry and panicking instead of failing gracefully. Fix by moving the counter increments to after all allocations succeed, so the struct is always consistent on any error path.	2026-08-15	7.8	CVE-2026-72485
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: PCI: Check ROM header and data structure <code>addr</code> before accessing We meet a crash when running stress-ng on x86_64 machine: BUG: unable to handle page fault for address: ffa0000007f40000 RIP: 0010:pci_get_rom_size+0x52/0x220 Call Trace: <TASK> pci_map_rom+0x80/0x130 pci_read_rom+0x4b/0xe0 kernfs_file_read_iter+0x96/0x180 vfs_read+0x1b1/0x300 Our analysis reveals that the ROM space's start address is 0xffa0000007f30000, and size is 0x10000. Because of broken ROM space, before calling <code>readl(pds)</code> , the <code>pds</code> 's value is 0xffa0000007f3ffff, which is already pointed to the ROM space end, invoking <code>readl()</code> would read 4 bytes therefore cause an out-of-bounds access and trigger a crash. Fix this by adding image header and data structure checking. We also found another crash on arm64 machine: Unable to handle kernel paging request at virtual address ffff8000dd1393ff Mem abort info: ESR = 0x0000000096000021 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x21: alignment fault The call trace is the same with x86_64, but the crash reason is that the data structure <code>addr</code> is not aligned with 4, and arm64 machine report "alignment fault". Fix this by adding alignment checking. [bhelgaas: shorten function names, wrap comments]	2026-08-15	7.7	CVE-2026-72487
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: soundwire: fix bug in <code>sdw_add_element_group_count</code> found by syzkaller The original implementation caused an out-of-bounds memory access in the <code>sdw_add_element_group_count</code> for-loop when <code>i == num</code> . for (<code>i = 0</code> ; <code>i <= num</code> ; <code>i++</code>) { if (<code>rate == group->rates[i]</code> && <code>lane == group->lanes[i]</code>) ... To fix this error, the function now checks for existing <code>rate/lane</code> entries in the group(a function	2026-08-15	7.8	CVE-2026-72488

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter) using a for-loop before adding them. No functional changes apart from this fix.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: ipv6: clamp default adverting MSS to avoid GSO_BY_FRAGS (0xFFFF) When MTU is large, ip6_default_advmss() can return IPV6_MAXPLEN (65535). This is interpreted by TCP as mss_clamp, allowing the MSS to reach 65535. However, 0xFFFF is also used as a magic value GSO_BY_FRAGS in the kernel. If a TCP packet with gso_size=0xFFFF is passed to skb_segment(), it will be mistakenly treated as GSO_BY_FRAGS, leading to a NULL pointer dereference because local TCP packets do not use frag_list. Fix this by returning min(IPV6_MAXPLEN, GSO_BY_FRAGS - 1) (65534) from ip6_default_advmss() when MTU is large. Also update the stale comment in ip6_default_advmss() which suggested that IPV6_MAXPLEN is returned to mean "any MSS".	2026-08-15	7.5	CVE-2026-72502
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sockmap: Fix use-after-free in udp_bpf_rcvmsg() syzbot reported use-after-free of struct sk_msg in sk_msg_rcvmsg(). [0] sk_msg_rcvmsg() peeks sk_msg from psock->ingress_msg under a lock, but its processing is lockless. Thus, sk_msg_rcvmsg() must be serialised by callers, otherwise multiple threads could touch the same sk_msg. For example, TCP uses lock_sock(), and AF_UNIX uses unix_sk(sk)->iolock. Initially, udp_bpf_rcvmsg() had used lock_sock(), but the cited commit removed it. Let's serialise sk_msg_rcvmsg() with lock_sock() in udp_bpf_rcvmsg(). Note that holding spin_lock_bh(&sk->sk_receive_queue.lock) is not an option due to copy_page_to_iter() in sk_msg_rcvmsg(). [0]: BUG: KASAN: slab-use-after-free in sk_msg_rcvmsg+0xb54/0xc30 net/core/skmsg.c:428 Read of size 4 at addr ffff88814cdc0000 by task syz.0.24/6020 CPU: 1 UID: 0 PID: 6020 Comm: syz.0.24 Not tainted syzkaller #0 PREEMPT(full) Hardware name: Google Compute Engine/Google Compute Engine, BIOS Google 01/13/2026 Call Trace: <TASK> dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xba/0x230 mm/kasan/report.c:482 kasan_report+0x117/0x150 mm/kasan/report.c:595 sk_msg_rcvmsg+0xb54/0xc30 net/core/skmsg.c:428 udp_bpf_rcvmsg+0x4bd/0xe00 net/ipv4/udp_bpf.c:84 inet_rcvmsg+0x260/0x270 net/ipv4/af_inet.c:891 sock_rcvmsg_nosec net/socket.c:1078 [inline] sock_rcvmsg+0x1a8/0x270 net/socket.c:1100 __sys_rcvmsg+0x1e6/0x4a0 net/socket.c:2812 __sys_rcvmsg+0x215/0x590 net/socket.c:2854 do_rcvmsg+0x334/0x800 net/socket.c:2949 __sys_rcvmsg net/socket.c:3023 [inline] __do_sys_rcvmsg net/socket.c:3046 [inline] __se_sys_rcvmsg net/socket.c:3039 [inline] __x64_sys_rcvmsg+0x198/0x250 net/socket.c:3039 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe2/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7fb319f9aeb9 Code: ff c3 66 2e 0f 1f 84 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff f7 d8 64 89 01 48 RSP: 002b:00007fb31ad97028 EFLAGS: 00000246 ORIG_RAX: 000000000000012b RAX: ffffffffda RBX: 00007fb31a216090 RCX: 00007fb319f9aeb9 RDX: 0000000000000001 RSI: 0000200000000400 RDI: 0000000000000004 RBP: 00007fb31a008c1f R08: 0000000000000000 R09: 0000000000000000 R10: 0000000040000021 R11: 0000000000000246 R12: 0000000000000000 R13: 00007fb31a216128 R14: 00007fb31a216090 R15: 00007ffe21dd0a98 </TASK> Allocated by task 6019: kasan_save_stack mm/kasan/common.c:57 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:78 poison_kmalloc_redzone mm/kasan/common.c:398 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:415 kasan_kmalloc include/linux/kasan.h:263 [inline] __kmalloc_cache_noprof+0x3d1/0x6e0 mm/slub.c:5780 kmalloc_noprof include/linux/slab.h:957 [inline] kzalloc_noprof include/linux/slab.h:1094 [inline] alloc_sk_msg net/core/skmsg.c:510 [inline] sk_psock_skb_ingress_self+0x60/0x350 net/core/skmsg.c:612 sk_psock_verdict_apply net/core/skmsg.c:1038 [inline] sk_psock_verdict_rcv+0x7d9/0x8d0 net/core/skmsg.c:1236 udp_read_skb+0x73e/0x7e0 net/ipv4/udp.c:2045 sk_psock_verdict_data_ready+0x12d/0x550 net/core/skmsg.c:1257 __udp_enqueue_schedule_skb+0xc54/0x10b0 net/ipv4/udp.c:1789 __udp_queue_rcv_skb net/ipv4/udp.c:2346 [inline] udp_queue_rcv_one_skb+0xac5/0x19c0 net/ipv4/udp.c:2475 __udp4_lib_mcast_deliver+0xc06/0xc0f net/ipv4/udp.c:2585	2026-08-15	7.8	CVE-2026-74257

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	__udp4_lib_rcv+0x10f6/0x2620 net/ipv4/udp.c:2724 ip_protocol_deliver_rcu+0x282/0x440 net/ipv4/ip_input.c:207 ip_local_deliver_finish+0x3bb/0x6f0 net/ipv4/ip_input.c:241 NF_HOOK+0x336/0x3c0 include/linux/netfilter.h:318 dst_input include/net/dst.h:474 [inline] ip_sublist_rcv_finish+0x221/0x2a0 net/ipv4/ip_input.c:584 ip_list_rcv_finish net/ipv4/ip_inp ---truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Guard __get_user access with access_ok for uprobe_multi data As reported by sashiko [1] we need to use access_ok to check the user space data bounds before we use __get_user to get it. [1] https://lore.kernel.org/bpf/20260610145235.CB1441F00893@smtp.kernel.org/	2026-08-15	7.8	CVE-2026-74258
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_dup_netdev: add nf_dev_xmit_recursion*() helpers and use them Update nft_dup and nft_fwd to use the nf_dev_xmit_recursion() helpers. This patch also disables BH when transmitting the skb to address a possible migration to different CPU leading to imbalanced decrementation of the recursion counters. This is modeled after Florian Westphal's dev_xmit_recursion*() API available since commit 97cdf37b57e ("net: place xmit recursion in softnet data") according to its current state in the tree.	2026-08-15	7.8	CVE-2026-74260
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: kcm: use WRITE_ONCE() when changing lower socket callbacks kcm_attach() replaces a live lower TCP socket's sk_data_ready and sk_write_space callbacks with KCM handlers, and kcm_unattach() restores them later. Those callback-pointer updates are still plain stores even though the same fields can be read and invoked concurrently on other CPUs. If another CPU observes an older callback snapshot after the live field has already been restored, callback execution can run with a mismatched target and sk_user_data state, leading to stale or misdirected wakeups. Use WRITE_ONCE() for the callback replacement and restore operations so these shared callback fields follow the same visibility contract already established by the earlier 4022 fixes.	2026-08-15	7.8	CVE-2026-74262
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: watchdog: fix refcount tracking races Blamed commit converted the untracked dev_hold()/dev_put() calls in the watchdog code to use the tracked dev_hold_track()/dev_put_track() (which were later renamed/interfaced to netdev_hold() and netdev_put()). By introducing dev->watchdog_dev_tracker to store the reference tracking information without adding synchronization between netdev_watchdog_up() and dev_watchdog(), it enabled the race condition where this pointer could be overwritten or freed concurrently, leading to the list corruption crash syzbot reported: list_del corruption, ffff888114a18c00->next is NULL kernel BUG at lib/list_debug.c:52 ! Oops: invalid opcode: 0000 [#1] SMP KASAN PTI CPU: 1 UID: 0 PID: 91 Comm: kworker/u8:5 Not tainted syzkaller #0 PREEMPT(lazy) Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 05/09/2026 Workqueue: events_unbound linkwatch_event RIP: 0010: __list_del_entry_valid_or_report.cold+0x22/0x2a lib/list_debug.c:52 Call Trace: <TASK> __list_del_entry_valid include/linux/list.h:132 [inline] __list_del_entry include/linux/list.h:246 [inline] list_move_tail include/linux/list.h:341 [inline] ref_tracker_free+0x1a7/0x6c0 lib/ref_tracker.c:329 netdev_tracker_free include/linux/netdevice.h:4491 [inline] netdev_put include/linux/netdevice.h:4508 [inline] netdev_put include/linux/netdevice.h:4504 [inline] netdev_watchdog_down net/sched/sch_generic.c:600 [inline] dev_deactivate_many+0x28c/0xfe0 net/sched/sch_generic.c:1363 dev_deactivate+0x109/0x1d0 net/sched/sch_generic.c:1397 linkwatch_do_dev net/core/link_watch.c:184 [inline] linkwatch_do_dev+0xd3/0x120 net/core/link_watch.c:166 __linkwatch_run_queue+0x3a5/0x810 net/core/link_watch.c:240 linkwatch_event+0x8f/0xc0 net/core/link_watch.c:314 process_one_work+0xa0e/0x1980 kernel/workqueue.c:3314 process_scheduled_works kernel/workqueue.c:3397 [inline] worker_thread+0x5ef/0xe50 kernel/workqueue.c:3478 kthread+0x370/0x450 kernel/kthread.c:436 ret_from_fork+0x69a/0xc80 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 This patch has three coordinated parts: 1) Add dev->watchdog_lock and dev->watchdog_ref_held to serialize watchdog operations. 2) Remove netdev_watchdog_up() call from netif_carrier_on(): This ensures netdev_watchdog_up() is only called from process/BH context (via linkwatch workqueue dev_activate()), allowing us to use spin_lock_bh() for synchronization. 3) Synchronize watchdog up and watchdog	2026-08-15	7.8	CVE-2026-74264

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	timer: Protect netdev_watchdog_up() with tx_global_lock and watchdog_lock. Only allocate a new tracker in netdev_watchdog_up() if one is not already present. In dev_watchdog(), ensure we don't release the tracker if the timer was rescheduled either by dev_watchdog() itself or concurrently by netdev_watchdog_up().			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: handshake: Require admin permission for DONE command ACCEPT and DONE are the two downcalls of the handshake genl family, both intended for use by the trusted handshake agent (tshd). ACCEPT already requires GENL_ADMIN_PERM; DONE has no privilege check at all. The fd-lookup in handshake_nl_done_doit() only confirms that some pending handshake request exists for the supplied sockfd; it does not authenticate the sender. An unprivileged process that guesses or observes a valid sockfd can therefore submit a DONE with HANDSHAKE_A_DONE_STATUS == 0, leaving the kernel consumer to proceed as if the handshake succeeded. A non-zero status on a forged DONE tears down a legitimate in-flight handshake before tshd can report its real result.	2026-08-15	7.8	CVE-2026-74270
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: reject inverted service ranges from peer bindings tipc_update_nametbl() inserts a binding advertised by a peer node using the lower and upper service-range bounds taken directly from the wire, without checking that lower <= upper. The local bind path validates the ordering (tipc_uaddr_valid()), but the name-distribution path does not. A binding with lower > upper is inserted at the far end of the service-range rbtree (keyed on lower) where no lookup or withdrawal can ever match it (service_range_foreach_match() requires sr->lower <= end). The publication, its service_range node and the augmented rbtree entry are then leaked for the lifetime of the namespace, and there is no per-peer cap equivalent to TIPC_MAX_PUBL on locally created bindings. Reject inverted ranges in the network path as well. A peer node can otherwise leak unbounded binding-table memory by sending PUBLICATION items with lower > upper.	2026-08-15	7.5	CVE-2026-74281
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: prevent snt_unacked underflow on CONN_ACK tipc_sk_conn_proto_rcv() subtracts the peer-supplied connection ack count from the unsigned 16-bit send counter snt_unacked without checking that it does not exceed the number of messages actually outstanding: tsk->snt_unacked -= msg_conn_ack(hdr); msg_conn_ack() is read straight from a received CONN_MANAGER/CONN_ACK message. If the ack count is larger than snt_unacked, the subtraction wraps to a near-maximum value, leaving tsk_conn_cong() permanently true and starving the connection of further transmits. Validate the ACK count at the start of the CONN_ACK block and drop the message if it acknowledges more messages than are outstanding. A peer (or, for a local connection, the connected peer socket) can otherwise wedge a TIPC connection's send side by sending an oversized connection ack.	2026-08-15	7.5	CVE-2026-74282
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: require net admin for TIPCv2 netlink mutators TIPCv2 registers mutating generic-netlink operations without admin permission flags. Generic netlink only checks CAP_NET_ADMIN when an operation sets GENL_ADMIN_PERM or GENL_UNSP_ADMIN_PERM, so a local unprivileged process can currently change TIPC state through commands such as TIPC_NL_NET_SET, TIPC_NL_KEY_SET, TIPC_NL_KEY_FLUSH, and bearer enable/disable. The legacy TIPC netlink API already checks netlink_net_capable(..., CAP_NET_ADMIN) for administrative commands. Give the TIPCv2 mutators the equivalent generic-netlink gate. Use GENL_UNSP_ADMIN_PERM, which maps to the same namespace-aware CAP_NET_ADMIN check that netlink_net_capable() performs, so the behaviour matches the legacy path and keeps working for CAP_NET_ADMIN holders in a non-initial user namespace (containers). A QEMU/KASAN repro run as uid/gid 65534 with zero effective capabilities previously succeeded in changing the network id and node identity, setting and flushing key material, and enabling/disabling a UDP bearer. With this patch applied the same operations fail with -EPERM.	2026-08-15	7.8	CVE-2026-74283
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: fib_rules: Don't dump dying fib_rule in fib_rules_dump(). rocker_router_fib_event() calls fib_rule_get() during RCU dump. If the fib_rule is dying, refcount_inc() will complain about it. Let's call refcount_inc_not_zero() in fib_rules_dump().	2026-08-15	7.8	CVE-2026-74288
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv4: fib: Don't dump dying fib_info in fib_leaf_notify(). syzbot reported use-after-free in nsim_fib4_prepare_event(). [0] The problem is that the following functions call	2026-08-15	7.8	CVE-2026-74289

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	fib_info_hold() / refcount_inc() while dumping fib_info under RCU, which is unsafe. * mlxsw_sp_router_fib4_event() * rocker_router_fib_event() * nsim_fib4_prepare_event() refcount_inc_not_zero() must be used, but it would be too late there. Let's guarantee the lifetime of fib_info in fib_leaf_notify(). Note that IPv6 does not need the corresponding change since fib6_table_dump() holds fib6_table.tb6_lock. [0]: refcount_t: addition on 0; use-after-free. WARNING: lib/refcount.c:25 at refcount_warn_saturate+0x9f/0x110 lib/refcount.c:25, CPU#0: kworker/u8:15/3420 Modules linked in: CPU: 0 UID: 0 PID: 3420 Comm: kworker/u8:15 Not tainted syzkaller #0 PREEMPT_{RT,(full)} Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/18/2026 Workqueue: netns cleanup_net RIP: 0010:refcount_warn_saturate+0x9f/0x110 lib/refcount.c:25 Code: eb 66 85 db 74 3e 83 fb 01 75 4c e8 1b f1 22 fd 48 8d 3d 84 cb f1 0a 67 48 0f b9 3a eb 4a e8 08 f1 22 fd 48 8d 3d 81 cb f1 0a <67> 48 0f b9 3a eb 37 e8 f5 f0 22 fd 48 8d 3d 7e cb f1 0a 67 48 0f RSP: 0018:ffffc9000f2c7270 EFLAGS: 00010293 RAX: ffffffff84a18858 RBX: 0000000000000002 RCX: ffff888032ff9ec0 RDX: 0000000000000000 RSI: 0000000000000000 RDI: ffffffff8f9353e0 RBP: 0000000000000000 R08: ffff888032ff9ec0 R09: 0000000000000005 R10: 0000000000000100 R11: 0000000000000004 R12: ffff8880570cc000 R13: dffffc0000000000 R14: ffff88802b40563c R15: ffff8880570cc000 FS: 0000000000000000(0000) GS:ffff888126173000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fb1f4d5d000 CR3: 000000006072a000 CR4: 00000000003526f0 Call Trace: <TASK> __refcount_add include/linux/refcount.h:-1 [inline] __refcount_inc include/linux/refcount.h:366 [inline] refcount_inc include/linux/refcount.h:383 [inline] fib_info_hold include/net/ip_fib.h:629 [inline] nsim_fib4_prepare_event drivers/net/netdevsim/fib.c:930 [inline] nsim_fib_event_schedule_work drivers/net/netdevsim/fib.c:1000 [inline] nsim_fib_event_nb+0x1055/0x1240 drivers/net/netdevsim/fib.c:1043 call_fib_notifier+0x45/0x80 net/core/fib_notifier.c:25 call_fib_entry_notifier net/ipv4/fib_trie.c:90 [inline] fib_leaf_notify net/ipv4/fib_trie.c:2176 [inline] fib_table_notify net/ipv4/fib_trie.c:2194 [inline] fib_notify+0x36b/0x5e0 net/ipv4/fib_trie.c:2217 fib_net_dump net/core/fib_notifier.c:70 [inline] register_fib_notifier+0x184/0x360 net/core/fib_notifier.c:108 nsim_fib_create+0x85d/0x9f0 drivers/net/netdevsim/fib.c:1596 nsim_dev_reload_create drivers/net/netdevsim/dev.c:1604 [inline] nsim_dev_reload_up+0x374/0x7c0 drivers/net/netdevsim/dev.c:1058 devlink_reload+0x501/0x8d0 net/devlink/dev.c:475 devlink_pernet_pre_exit+0x1ff/0x420 net/devlink/core.c:558 ops_pre_exit_list net/core/net_namespace.c:161 [inline] ops_undo_list+0x187/0x940 net/core/net_namespace.c:234 cleanup_net+0x56e/0x800 net/core/net_namespace.c:702 process_one_work kernel/workqueue.c:3314 [inline] process_scheduled_works+0xb5d/0x1860 kernel/workqueue.c:3397 worker_thread+0xa53/0xfc0 kernel/workqueue.c:3478 kthread+0x388/0x470 kernel/kthread.c:436 ret_from_fork+0x514/0xb70 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK>			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: tegra: tegra210_ahub: Validate written enum value tegra_ahub_put_value_enum() reads e->values[item[0]] before checking whether item[0] is within the enum item range. The existing check therefore happens too late to prevent an out-of-range read of the values array. Move the check before the array access.	2026-08-15	7.1	CVE-2026-74292
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: fsl: fsl_audmix: Validate written enum values fsl_audmix_put_mix_clk_src() and fsl_audmix_put_out_src() convert the user-provided enum item with snd_soc_enum_item_to_val() before checking whether the item is within the enum's item count. The generic snd_soc_put_enum_double() helper performs that validation, but these callbacks use the converted value first: the clock-source path tests it with BIT(), and the output-source path indexes the prms transition table with it. Reject out-of-range enum items before converting them.	2026-08-15	7.8	CVE-2026-74293
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: meson: aiu: Validate written enum values The AIU HDMI and internal codec mux put callbacks use the written enum value with snd_soc_enum_item_to_val() before checking whether the value is valid for the enumeration. Reject out-of-range values before converting the enum item, matching the validation already done by the G12A HDMI and internal codec mux controls.	2026-08-15	7.3	CVE-2026-74294

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: hdac_hdmi: Validate written enum value hdac_hdmi_set_pin_port_mux() uses the written enum value to index the texts array before calling snd_soc_dapm_put_enum_double(), which validates that the value is within the enum item range. An out-of-range value can therefore make the driver read past the texts array before the helper rejects the write. Move the lookup after the helper has accepted the value.	2026-08-15	7.1	CVE-2026-74295
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Release the HW provided UAR index rather than the SW one Free the UAR index returned by the hardware.	2026-08-15	7.8	CVE-2026-74296
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix undefined shift of user RQ WQE size set_rq_size() computes the RQ WQE size as "1 << rq_wqe_shift" based on the user-provided rq_wqe_shift, which is only checked to be greater than 32, so shifts of 32 are still accepted. A shift of 31 also overflows a signed integer, leading to undefined behavior. Use check_shl_overflow() to compute the RQ WQE size and reject any invalid values.	2026-08-15	7.8	CVE-2026-74297
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_core: Fix UAF in hci_unregister_dev() hci_unregister_dev() does not disable cmd_timer and ncmd_timer before the hci_dev structure is freed. If a timeout fires during device teardown, the callback dereferences freed memory (including the hdev->reset function pointer), leading to a use-after-free. Add disable_delayed_work_sync() calls alongside the existing disable_work_sync() calls to ensure both timers are fully quiesced before teardown proceeds.	2026-08-15	7.8	CVE-2026-74302
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Tighten cgroup storage cookie checks for prog arrays The fix in commit abad3d0bad72 ("bpf: Fix oob access in cgroup local storage") is still incomplete. The prog-array compatibility check treats a program with no cgroup storage as compatible with any stored storage cookie. This allows a storage-less program to bridge a tail call chain between an entry program and a storage-using callee even though cgroup local storage at runtime still follows the caller's context, that is, A -> B(no storage) -> C(storage) path. Requiring exact cookie equality would break the legitimate case of a storage-less leaf program being tail called from a storage-using one. Instead, only accept a zero storage cookie if the program cannot perform tail calls itself. This keeps A -> B(no storage) working while rejecting the A -> B(no storage) -> C(storage) bridge.	2026-08-15	7.8	CVE-2026-74305
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vfio/qat: fix f_pos race in qat_vf_resume_write() qat_vf_resume_write() checks filp->f_pos before taking migf->lock, but copies into the migration-state buffer after taking the lock and re-reading the shared file position. Two concurrent writers could therefore pass the bounds check with the old offset, then have the second writer copy after the first advanced f_pos, writing past the end of the migration-state buffer. Take migf->lock before doing the boundary checks.	2026-08-15	7.8	CVE-2026-74306
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: virtio: rtc: tear down old virtqueues before restore virtio_device_restore() resets the device and restores the negotiated features before calling ->restore(). viortc_freeze() intentionally leaves the existing virtqueues in place so the alarm queue can still wake the system, but viortc_restore() immediately calls viortc_init_vqs() without first deleting those old queues. If virtqueue reinitialization fails on virtio-pci, the transport error path can run vp_del_vqs() against a newly allocated vp_dev->vqs array while vdev->vqs still contains the old virtqueues. vp_del_vqs() then looks up queue state through the new array and can dereference a NULL info pointer in vp_del_vq(), crashing the guest kernel during restore. This can also happen during a non-faulty reinitialization, when one of the vp_find_vqs_msix() attempts is unsuccessful before a later attempt would succeed. Delete the stale virtqueues before rebuilding them. If restore fails before virtio_device_ready(), reuse the remove path to stop the device. Once the device is ready, return errors directly instead of deleting the virtqueues again.	2026-08-15	7.8	CVE-2026-74311
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vhost/vdpa: validate virtqueue index in mmap and fault paths vhost_vdpa_mmap() and vhost_vdpa_fault() use vma->vm_pgoff as a virtqueue index for get_vq_notification(), but they do not validate that the index is smaller than v->nvqs. The ioctl path already performs both a bounds check and array_index_nospec(), but the mmap/fault path only checks that the index fits in u16. This allows an out-of-range queue index to reach driver-specific	2026-08-15	7.8	CVE-2026-74312

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	get_vq_notification() callbacks. Fix this by extracting a unified vhost_vdpa_get_vq_notification() helper that validates the queue index against v->nvqs and applies array_index_nospec() before calling the driver callback. Both the mmap and fault paths use this helper, and the bounds checking is consolidated into a single location. From source inspection, the most defensible impact is out-of-bounds access in the callback path, potentially leading to invalid PFN remaps and crash/DoS.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Cancel special fields on map value recycle Map update and delete paths currently call bpf_obj_free_fields() when a value is being replaced or recycled. That makes field destruction depend on the context of the update/delete operation. For tracing programs this can include NMI context, where referenced kptr destructors, uptr unpinning, and graph root destruction are not generally safe. Introduce bpf_obj_cancel_fields() for the reusable-value path. It only performs NMI-safe cleanup for timer, workqueue, and task_work fields. Fields that need full destruction are left attached to the recycled value and are destroyed by the final cleanup path instead. Switch array and hashtable update/delete/recycle paths to this cancel helper. Keep bpf_obj_free_fields() for final map destruction and for bpf_mem_alloc destructors. Preallocated hashtabs do not have allocator destructors, so teardown continues to walk the normal and extra elements and fully destroy their fields. This deliberately relaxes the eager-free semantics of map update/delete for special fields. Programs that relied on a recycled map slot becoming empty immediately after update/delete were relying on behavior that cannot be implemented safely from every BPF execution context without offloading arbitrary destructors. There is a chance this change breaks programs making assumptions regarding the eager freeing of fields. If so, we can relax semantics to cancellation only when irq_disabled() is true in the future. However, theoretically, map values that get reused eagerly already have weaker guarantees as parallel users can recreate freed fields before the new element becomes visible again.	2026-08-15	7.8	CVE-2026-74314
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: NFSD: Handle layout stid in nfsd4_drop_revoked_stid() nfsd4_drop_revoked_stid() has no SC_TYPE_LAYOUT case, so when a client sends FREE_STATEID for an admin-revoked layout stid, the default branch releases cl_lock and returns without unhashing or releasing the stid. The stid remains in the IDR and on the per-client list until the client is destroyed. Remove the layout stid from the per-client list and call nfs4_put_stid() to drop the creation reference. When the refcount reaches zero, nfsd4_free_layout_stateid() handles the remaining cleanup: cancelling the fence worker, removing from the per-file list, and freeing the slab object.	2026-08-15	7.5	CVE-2026-74316
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ixgbe: do not configure xps for XDP queues netif_set_xps_queue() should not be called for an XDP Tx queue, since such queues are not netdev-exposed. On systems with number of CPUs >=64, on E610 adapter, netdev is configured with maximum number queue pairs being 63 (due to MSI-X assignment), but configuring XDP results in 64 XDP queues. So, during XDP program load, when netif_set_xps_queue() is called for the last XDP queue, we get a WARNING with a call trace and KASAN report afterwards (if enabled). [2012.699800] WARNING: net/core/dev.c:2854 at __netif_set_xps_queue+0x116a/0x1e40, CPU#36: xdpsock/103668 [...] [2012.700029] RIP: 0010: __netif_set_xps_queue+0x116a/0x1e40 [2012.700035] Code: b6 34 06 48 89 f8 83 e0 07 83 c0 01 40 38 f0 7c 09 40 84 f6 0f 85 03 0a 00 00 0f b7 44 24 40 66 43 89 44 6a 18 e9 01 fb ff ff <0f> 0b e9 f2 ee ff ff 44 8b 44 24 44 45 85 c0 74 50 4d 85 e4 0f 84 [2012.700040] RSP: 0018:ffff8882369aeb28 EFLAGS: 00010246 [2012.700046] RAX: 0000000000000000 RBX: 000000000000003f RCX: 0000000000000000 [2012.700050] RDX: 1ffff111da3d891 RSI: ffff888120e34250 RDI: ffff8888ed1ec488 [2012.700054] RBP: ffff888913281560 R08: 0000000000000000 R09: ffff8888ed1ec000 [2012.700058] R10: ffff8888a2e83180 R11: 0000000000000000 R12: 0000000000007fa8 [2012.700061] R13: 000000000000003f R14: ffff888120e34854 R15: ffff8889132817c8 [2012.700065] FS: 00007fc8ea9ff740(0000) GS:ffff8884cefe0000(0000) knlGS:0000000000000000 [2012.700069] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [2012.700073] CR2: 00007f81c8000020 CR3: 00000002299f8006 CR4: 00000000007726f0 [2012.700077] PKRU: 55555554 [2012.700080] Call Trace: [2012.700084] <TASK> [2012.700087] ? ktime_get+0x61/0x150 [2012.700097] ? usleep_range_state+0x133/0x1b0 [2012.700108] ?	2026-08-15	7.8	CVE-2026-74317

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	__pfx_usleep_range_state+0x10/0x10 [2012.700114] netif_set_xps_queue+0x31/0x50 [2012.700119] ixgbe_configure_tx_ring+0x472/0x920 [ixgbe] [...] [2012.700486] ixgbe_xdp+0x38f/0x750 [ixgbe] [...] [2012.701094] BUG: KASAN: slab-out-of-bounds in __netif_set_xps_queue+0x1ac5/0x1e40 [2012.701100] Write of size 4 at addr ffff88888d43cff8 by task xdpsock/103668 Skip XPS configuration for XDP Tx queues.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix invalid pointer dereference in __btrfs_run_delayed_refs() In the beginning of the loop, we try to obtain a locked delayed ref head, if 'locked_ref' is currently NULL, by calling btrfs_select_ref_head(), which can return an error pointer. If the error pointer is -EAGAIN we do a continue and go back to the beginning of the loop, which will not try again to call btrfs_select_ref_head() since 'locked_ref' is no longer NULL but it's ERR_PTR(-EAGAIN), and then we do: spin_lock(&locked_ref->lock); against a ERR_PTR(-EAGAIN) value, generating an invalid pointer dereference. Fix this by ensuring that 'locked_ref' is set to NULL when btrfs_select_ref_head() returns ERR_PTR(-EAGAIN) and incrementing 'count' as well, to prevent infinite looping. We do this by doing a goto to the bottom of the loop that already sets 'locked_ref' to NULL and does a cond_resched(), with an increment to 'count' right before the goto. These measures were in place before the refactoring in commit 0110a4c43451 ("btrfs: refactor __btrfs_run_delayed_refs loop") but were unintentionally lost afterwards.	2026-08-15	7.5	CVE-2026-74321
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: use kfree_rcu for offchannel link in mt76_put_vif_phy_link mt76_put_vif_phy_link() frees the offchannel mlink with plain kfree() after rcu_assign_pointer(NULL). However, rcu_assign_pointer only prevents future RCU readers from obtaining the pointer -- it does not wait for existing readers that already hold it via rcu_dereference. The TX datapath (e.g. mt7996_mac_write_txwi) dereferences mlink->wcid and mlink->idx under rcu_read_lock. If a TX softirq obtained the pointer via rcu_dereference just before the NULL assignment, it will dereference freed memory after the kfree. struct mt76_vif_link already contains an rcu_head field that is unused at this free site -- a developer oversight, since the adjacent kfree_rcu_mightsleep call for rx_sc in the same function shows the pattern was understood. Replace kfree(mlink) with kfree_rcu(mlink, rcu_head).	2026-08-15	7.8	CVE-2026-74325
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: configfs: fix lockless traversals of ->s_children Having the parent directory locked protects entries from removal by another thread, but it does *not* protect cursors from being moved around by lseek() - or freed, for that matter.	2026-08-15	7.8	CVE-2026-74330
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/nldev: Fix locking when accessing mr->pd Sashiko points out that, due to rereg_mr, the PD is actually variable and all the touches in nldev are racy. Use mr->device instead of mr->pd->device. Getting the PD restrack ID is more tricky. To avoid disturbing all the happy paths, add an rdma_restrack_sync() operation which is sort of like flush_workqueue() or synchronize_irq(): after it returns, all the old nldev touches to the mr are gone and everything sees the new PD. This makes it safe to reach into the PD pointer.	2026-08-15	7.8	CVE-2026-74334
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject sleepable BPF_LSM_CGROUP programs at load time The cgroup shim runs under rcu_read_lock_dont_migrate(), so we should not attach any sleepable BPF programs there. Add support to the verifier to explicitly reject attempts to load sleepable BPF programs destined for LSM cgroup attachment. Without this, we get the following splat from a BPF_LSM_CGROUP program marked BPF_F_SLEEPABLE attached to file_open when it calls bpf_get_dentry_xattr(): BUG: sleeping function called from invalid context at kernel/locking/rwsem.c:1567 in_atomic(): 0, irqs_disabled(): 0, non_block: 0, pid: 34317, name: load preempt_count: 0, expected: 0 RCU nest depth: 2, expected: 0 Call Trace: down_read+0x76/0x480 ext4_xattr_get+0x11f/0x700 __vfs_getxattr+0xf0/0x150 bpf_get_dentry_xattr+0xbb/0xf0 bpf_prog_e76a298dac9218c6_test_open+0x6a/0x85 __cgroup_bpf_run_lsm_current+0x326/0x840 bpf_trampoline_6442534646+0x62/0x14d security_file_open+0x34/0x60 do_dentry_open+0x340/0x1260 vfs_open+0x7a/0x440 path_openat+0x1bac/0x30a0 libbpf provides a .s named section variant for every sleepable program type except lsm_cgroup, reflecting that per-cgroup LSM	2026-08-15	7.8	CVE-2026-74338

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	programs are intended to only run in a non-sleepable context. The above splat was obtained by bypassing libbpf by using bpf(2) directly.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: kernfs: fix xattr race condition with multiple superblocks Multiple superblocks with different namespaces can share the same kernfs_node when kernfs_test_super() finds a matching root but different namespace. This means multiple inodes from different superblocks can reference the same kernfs_node->iattr->xattrs structure. The VFS layer only holds per-inode locks during xattr operations, which is insufficient to serialize concurrent xattr modifications on the shared kernfs_node. This can lead to race conditions in simple_xattr_set() where the lookup->replace/remove sequence is not atomic with respect to operations from other superblocks. Fix this by protecting xattr operations with the existing hashed kernfs_locks->open_file_mutex[] array, which is already used to protect per-node open file data. The hashed mutex array provides scalable per-node serialization (scaled by CPU count, up to 1024 locks on 32+ CPU systems) with zero memory overhead. Changes: - Rename open_file_mutex[] to node_mutex[] to reflect dual purpose - Add kernfs_node_lock_ptr() and kernfs_node_lock() helpers - Protect simple_xattr_set() calls in kernfs_xattr_set() and kernfs_vfs_user_xattr_set() with the hashed mutex - Update file.c to use new helpers via compatibility wrappers - Update documentation to explain the extended lock usage	2026-08-15	7.8	CVE-2026-74343
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Clear rb node linkage when freeing bpf_rb_root bpf_rb_root_free() detaches the root by copying the current rb_root_cached and then replacing the live root with RB_ROOT_CACHED. It then walks the copied root and drops each object contained in the tree. This leaves the rb node state intact while dropping the object. If the object is refcounted and survives the drop, its bpf_rb_node_kern still contains an owner pointer to the freed root and stale rb tree linkage. If a later bpf_rb_root allocation reuses the same address, bpf_rbtrees_remove() can incorrectly pass the owner check and call rb_erase_cached() on a node whose rb pointers belong to the old tree. Mirror the list draining behavior by marking nodes as busy while the root is being detached, then clear the rb node and release the owner before dropping the containing object. This makes surviving nodes unowned and safe to reject from remove or accept for a later add.	2026-08-15	7.8	CVE-2026-74344
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: cttimetypeout: detach dataplane timeout policy and repurpose refcount Add a refcount for struct nf_ct_timeout which is used by ct extension to set the custom ct timeout policy, this tells us that the ct timeout is being used by a conntrack entry. When the last conntrack entry drops the refcount on the ct timeout, the ct timeout is released. Remove the refcount for control plane which controls if the ruleset refers to the timeout policy. After this update, it is possible to remove the ct timeout policy from nfnetlink_cttimetypeout immediately. This is for simplicity not to handle two refcounts on a single object. Remove nf_queue_nf_hook_drop(): a packet sitting in nfqueue will just hold a reference to the nf_ct_timeout object until packet is reinjected, since this is part of the ct extension, this will be released by the time the conntrack is freed. nf_ct_untimeout() is still called to clean up in a best effort basis: the ct timeout on existing entries gets removed when the ct timeout goes away, but as long as the iptables ruleset still refers to the ct timeout through a template, new conntracks may keep attaching it and extend its lifetime until the rule is removed. nf_ct_untimeout() is not called anymore from module removal path, this is unlikely to find timeouts give module refcount is bumped, and the new refcount already tracks the ct timeout policy use so it is released when unused.	2026-08-15	7.8	CVE-2026-74347
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: reject FITRIM ranges shorter than a cluster ocfs2_trim_mainbm() trims the global bitmap in cluster units, but its too-short range validation only checks sb->s_blocksize. On filesystems with a cluster size larger than the block size, a FITRIM range that is at least one block but shorter than one cluster is accepted and shifted down to len == 0. The later start + len - 1 and len -= ... arithmetic then underflows and can drive trimming past the requested range. Reject ranges shorter than s_clustersize instead. That preserves the existing -EINVAL behavior for requests that cannot discard even one allocation unit and keeps zero-cluster trims out of the group walk.	2026-08-15	7.1	CVE-2026-74349
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Take mmap_lock in zap_pages() zap_vma_range() requires the owning mm's mmap_lock to be held. Taking mmap_read_lock under arena->lock would AB-BA against arena_vm_close() and arena_map_mmap(), both of which run with mmap_write_lock held and then acquire arena->lock. Instead drop arena->lock,	2026-08-15	7.8	CVE-2026-74354

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mmget_not_zero() the vma's mm, take mmap_read_lock, and re-resolve the vma via find_vma() since it may have been unmapped or replaced while waiting. Track processed vmls with a per-call generation in vml->zap_gen and serialize zap_pages() callers with a new arena->zap_mutex so concurrent callers on different uaddr ranges do not mark each other's vmls processed before the zap is done.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vhost: fix vhost_get_avail_idx for a non empty ring vhost_get_avail_idx is supposed to report whether it has updated vq->avail_idx. Instead, it returns whether all entries have been consumed, which is usually the same. But not always - in drivers/vhost/net.c and when mergeable buffers have been enabled, the driver checks whether the combined entries are big enough to store an incoming packet. If not, the driver re-enables notifications with available entries still in the ring. The incorrect return value from vhost_get_avail_idx propagates through vhost_enable_notify and causes the host to livelock if the guest is not making progress, as vhost will immediately disable notifications and retry using the available entries. This goes back to commit d3bb267bbdcb ("vhost: cache avail index in vhost_enable_notify()") which changed vhost_enable_notify() to compare the freshly read avail index against vq->last_avail_idx instead of the previously cached vq->avail_idx. Commit 7ad472397667 ("vhost: move smp_rmb() into vhost_get_avail_idx()") then carried over the same comparison when refactoring vhost_enable_notify() to call the unified vhost_get_avail_idx(). The obvious fix is to make vhost_get_avail_idx do what the comment says it does and report whether new entries have been added.	2026-08-15	7.4	CVE-2026-74356
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix KASAN slab-out-of-bounds in amdgpu_coredump ring dump The ring content dump in amdgpu_coredump() uses two separate loops over adev->rings[]: the first counts rings with unsignalled fences to size the allocation, and the second copies ring data into the allocated buffers. Both loops use the same condition to skip rings: atomic_read(&ring->fence_drv.last_seq) == ring->fence_drv.sync_seq Because last_seq is an atomic that is updated concurrently by the fence signalling path, additional rings may appear unsignalled in the second loop that were signalled during the first. When this happens, idx exceeds the allocated ring_count and the store to coredump->rings[idx] writes past the end of the kalloc-ed buffer. This was found during IGT stressful test amd_queue_reset which triggers random GPU resets. The OVERSIZE subtest (CMD_STREAM_EXEC_INVALID_PACKET_LENGTH_OVERSIZE on GFX ring) provokes a ring timeout and subsequent coredump, which hits the race between the counting and copying loops. The failure is non-deterministic and depends on fence signalling timing during the reset. KASAN log: BUG: KASAN: slab-out-of-bounds in amdgpu_coredump+0x1274/0x12f0 [amdgpu] Write of size 4 at addr ffff888106154258 by task kworker/u128:5/23625 CPU: 16 UID: 0 PID: 23625 Comm: kworker/u128:5 Not tainted 6.19.0+ #35 Workqueue: amdgpu-reset-dev drm_sched_job_timeout [gpu_sched] Call Trace: <TASK> dump_stack_lvl+0xa5/0x110 print_report+0xd1/0x660 kasan_report+0xf3/0x130 __asan_report_store4_noabort+0x17/0x30 amdgpu_coredump+0x1274/0x12f0 [amdgpu] amdgpu_job_timeout+0xef0/0x16c0 [amdgpu] drm_sched_job_timeout+0x194/0x5c0 [gpu_sched] process_one_work+0x84b/0x1990 worker_thread+0x6b8/0x11b0 </TASK> Allocated by task 23625: kasan_save_stack+0x39/0x70 __kasan_kmalloc+0xc3/0xd0 __kmalloc_noprof+0x2ec/0x910 amdgpu_coredump+0x5c5/0x12f0 [amdgpu] amdgpu_job_timeout+0xef0/0x16c0 [amdgpu] The buggy address belongs to the object at ffff888106154200 which belongs to the cache kmalloc-rnd-09-96 of size 96 The buggy address is located 16 bytes to the right of allocated 72-byte region [ffff888106154200, ffff888106154248) 72 bytes = 3 * sizeof(struct amdgpu_coredump_ring), so ring_count was 3 but idx reached 3+, writing ring_index (at struct offset 16) 16 bytes past the allocation. Fix by adding an idx < ring_count guard to the copy loop so it cannot exceed the allocated count even when the fence state changes between the two passes.	2026-08-15	7.8	CVE-2026-74357
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: configs_lookup(): don't leave ->s_dentry dangling on failure Normally ->s_dentry is cleared when dentry it's pointing to becomes negative (on eviction, realistically). However, that only happens if dentry gets to be positive in the first place; in case of inode allocation failure dentry never becomes positive, so ->d_iput() is not called at	2026-08-15	7.8	CVE-2026-74359

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	all. We do part of what normally would've been done by configfs_d_iput() (dropping the reference to configfs_dirent) manually, but we do not clear ->s_dentry there. Sloppy as it is, it does not matter in case of configfs_create_{dir,link}() - there configfs_dirent does not survive dropping the sole reference to it. However, for configfs_lookup() it *does* survive, with a dangling pointer to soon to be freed dentry sitting it its ->s_dentry. Subsequent getdents(2) in that directory will end up dereferencing that pointer in order to pick the inode number. Use after free... This is the minimal fix; the right approach is to set the linkage between dentry and configfs_dirent only after we know that we have an inode, but that takes more surgery and the bug had been there since 2006, so...			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: fix UAF by restoring RCU-delayed inode freeing in bpf commit 4f375ade6aa9 ("bpf: Avoid RCU context warning when unpinning htab with internal structs") moved inode cleanup from ->free_inode() into ->destroy_inode() to avoid sleeping in RCU context when calling bpf_any_put(). However this removed the RCU delay on freeing the inode itself and the cached symlink body (i_link), both of which can be accessed by RCU pathwalk (pick_link, may_lookup etc.). This causes a use-after-free when a concurrent unlinkat() drops the last inode reference and destroy_inode() frees the inode immediately, while another task is still walking the path in RCU mode and reads inode->i_opflags (offset +2) inside current_time() -> is_mgtime(). KASAN reports: BUG: KASAN: slab-use-after-free in is_mgtime include/linux/fs.h:2313 Read of size 2 at addr ffff8880407e4282 (offset +2 = i_opflags) The rules (per Al Viro): ->destroy_inode() called immediately, can sleep, use for blocking cleanup e.g. bpf_any_put() ->free_inode() called after RCU grace period, use for freeing inode and anything RCU-accessible e.g. i_link Fix: split the two concerns properly: - keep bpf_any_put() in bpf_destroy_inode() since it is blocking and needs to run promptly - introduce bpf_free_inode() to handle kfree(i_link) and free_inode_nonrcu() with proper RCU delay, preventing the UAF	2026-08-15	7.8	CVE-2026-74363
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject exclusive maps as inner maps in map-in-map An exclusive map (created with excl_prog_hash) is bound to a single program by hash: check_map_prog_compatibility() refuses to load any program whose digest does not match map->excl_prog_sha. That check only runs for maps a program references directly, i.e. its used_maps. A map reached at runtime through a map-of-maps is never in used_maps, and bpf_map_meta_equal() does not consider excl_prog_sha, so an exclusive map can be inserted into a non-exclusive outer map and then looked up and mutated by an unrelated program, bypassing the exclusivity guarantee. For the signed loader this defeats the metadata map exclusivity check added in the signed loader: the cached map->sha[] is validated against the signed hash while another program on a hostile host rewrites the frozen map's contents through the outer map.	2026-08-15	7.1	CVE-2026-74364
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvdim/btt: Handle preemption in BTT lane acquisition BTT lanes serialize access to per-lane metadata and workspace state during BTT I/O. The btt-check unit test reports data mismatches during BTT writes due to a race in lane acquisition that can lead to silent data corruption. The existing lane model uses a spinlock together with a per-CPU recursion count. That recursion model stopped being valid after BTT lanes became preemptible: another task can run on the same CPU, observe a non-zero recursion count, bypass locking, and use the same lane concurrently. BTT lanes are also held across arena_write_bytes() calls. That path reaches nsio_rw_bytes(), which flushes writes with nvdim_flush(). Some provider flush callbacks can sleep, making a spinlock the wrong primitive for the lane lifetime. Replace the spinlock-based recursion model with a dynamically allocated per-lane mutex array and take the lane lock unconditionally. Add might_sleep() to catch any future atomic-context caller. Found with the ndctl unit test btt-check.sh.	2026-08-15	7.3	CVE-2026-74365
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix inconsistent arvif state in vdev_create error paths ath12k_mac_vdev_create() has three error path issues that leave arvif in an inconsistent state: 1. When ath12k_wmi_vdev_create() fails, the function returns directly without clearing arvif->ar, which was already set before the WMI call. Subsequent code checking arvif->ar to determine vdev readiness will see a non-NULL value despite no vdev existing in firmware. 2. When ath12k_wmi_send_peer_delete_cmd() fails in err_peer_del, the code jumped to err: skipping the DP peer cleanup and vdev rollback, leaving num_created_vdevs, vdev maps and arvif list membership live. 3.	2026-08-15	7.8	CVE-2026-74367

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	When ath12k_wait_for_peer_delete_done() fails, the code jumped to err_vdev_del: skipping the DP peer cleanup. Fix by changing the ath12k_wmi_vdev_create() failure to goto err instead of returning directly, routing both err_peer_del failure paths through err_dp_peer_del: for proper DP peer and vdev rollback, and consolidating the arvif state cleanup at err:. Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.1.c5-00302-QCAHMTSWPL_V1.0_V2.0_SILICONZ-1.115823.3			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: fix BPF_PROG_QUERY OOB write and cgroup backward compat BPF_PROG_QUERY writes back the 'query.revision' field unconditionally to userspace. If userspace passes a smaller 'bpf_attr' structure (e.g. 40 bytes, which was the layout before the addition of 'query.revision'), the kernel performs an out-of-bounds write. Fix this by propagating the user-provided attribute size 'uattr_size' down to the cgroup query handlers, and conditionally skipping writing the revision field to userspace when the provided buffer size is insufficient. query.revision in bpf_mprog_query is structurally identical to the cgroup case: a late tail field, written unconditionally. But the backward-compat hazard is not the same. The min-historical-size test is per command, and bpf_mprog_query only serves attach types that were born with revision in the struct: - tcx_prog_query -> BPF_TCX_INGRESS/EGRESS - netkit_prog_query -> BPF_NETKIT_PRIMARY/PEER tcx, netkit, the revision field, and bpf_mprog_query itself all landed in the same v6.6 merge window (053c8e1f235d added the mprog query API + revision; tcx in e420bed02507, netkit in 35dfaad7188c). There has never been a tcx/netkit BPF_PROG_QUERY userspace that doesn't know about revision. So for these commands the minimum legitimate struct already covers offset 56-64 - no old binary can be broken here. Contrast with cgroup: BPF_PROG_QUERY on cgroup attach types shipped in 2017; revision write-back was bolted on years later (120933984460). That path has a real population of pre-revision callers.	2026-08-15	7.8	CVE-2026-74371
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: md/raid1,raid10: fix error-path detection with md_cloned_bio() Detect the error path using md_cloned_bio() instead of relying on r1_bio in raid1 or r10_bio->read_slot in raid10, which may be NULL or -1 after splitting and resubmitting a failed bio. As a result, the error path may not be recognized and memory allocations can incorrectly use GFP_NOIO instead of (GFP_NOIO __GFP_HIGH), which can lead to a deadlock under memory pressure.	2026-08-15	7.5	CVE-2026-74374
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Copy WQE to local buffer in non-SRQ receive path For non-SRQ QPs, the responder reads WQE fields directly from the shared queue buffer mapped into userspace. This allows a malicious user to modify fields like num_sge or sge entries while the kernel is processing the WQE, leading to out-of-bounds reads in rxe_resp_check_length() and copy_data(). Introduce get_rcv_wqe() that validates num_sge and copies the WQE to a kernel-local buffer before processing, matching the approach already used for SRQ WQEs in get_srq_wqe(). The srq_wqe buffer is reused since SRQ and non-SRQ paths are mutually exclusive per QP.	2026-08-15	7.8	CVE-2026-74377
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix TOCTOU heap overflow in get_srq_wqe get_srq_wqe() reads wqe->dma.num_sge from the shared receive queue buffer, which is mapped into userspace. It validates num_sge against max_sge, but then re-reads the same field to calculate the memcpy size. A concurrent userspace thread can modify num_sge between validation and use, causing a heap buffer overflow when copying the WQE into qp->resp.srq_wqe. Read num_sge into a local variable and use it for both the bounds check and the size calculation.	2026-08-15	7.8	CVE-2026-74378
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: check return value of nvmet_tcp_set_queue_sock The return value of nvmet_tcp_set_queue_sock() is currently ignored in nvmet_tcp_tls_handshake_done(). If it fails (e.g., due to the socket not being in TCP_ESTABLISHED state), the socket callbacks will not be properly set, leading to queue and socket leakage. Fix this by capturing the return value and calling nvmet_tcp_schedule_release_queue() on failure to ensure proper cleanup.	2026-08-15	7.5	CVE-2026-74385
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: seq: midi: Serialize output teardown with event_input event_process_midi() borrows msynth->output_rfile.output and then passes the substream to dump_midi() and snd_rawmidi_kernel_write() without synchronizing with the output open/close transition. midisynth_use() also publishes output_rfile before	2026-08-15	7.8	CVE-2026-74387

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	snd_rawmidi_output_params() has finished. The last midisynth_unuse() can therefore release the same rawmidi file and free substream->runtime before snd_rawmidi_kernel_write1() takes its runtime buffer reference. That leaves the event_input path using a stale substream or runtime and can end in a NULL-deref or use-after-free. Fix this with two pieces of synchronization. Keep a short IRQ-safe spinlock only for publishing or clearing output_rfile and for pairing the output snapshot with an snd_use_lock_t reference. Once event_process_midi() has taken that in-flight reference, it drops the spinlock before calling snd_seq_dump_var_event(), dump_midi(), or snd_rawmidi_kernel_write(). midisynth_unuse() now detaches the visible rawmidi file under the same spinlock, waits for the in-flight writers to drain, and only then drains and releases the saved file. midisynth_use() likewise opens into a local snd_rawmidi_file and publishes it only after snd_rawmidi_output_params() succeeds. The buggy scenario involves two paths, with each column showing the order within that path: event_input path: last unuse path: 1. event_process_midi() snapshots 1. midisynth_unuse() starts output_rfile.output. tearing down output_rfile. 2. dump_midi() reaches 2. snd_rawmidi_kernel_release() snd_rawmidi_kernel_write() closes the output file. before runtime is pinned. 3. close_substream() frees 3. The callback keeps using substream->runtime. the borrowed substream. Validation reproduced this kernel report: KASAN null-ptr-deref in snd_rawmidi_kernel_write1+0x56/0x360 RIP: 0033:0x7fde7dd0837f RIP: 0010:snd_rawmidi_kernel_write1+0x56/0x360			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: seq: oss: Fix UAF at handling events with embedded SysEx data The OSS sequencer processes the input MIDI bytes into a sequencer event to be dispatched later (in snd_seq_oss_midi_putc() called from snd_seq_oss_process_event()). When it's a SysEx data, the event record contains data.ext.ptr pointer to the original SysEx bytes, and the referred data is copied into the pool afterwards at dispatching. The problem is that, if the sequencer port gets closed concurrently before the dispatch, the OSS sequencer core also releases the resources (in snd_seq_oss_midi_check_exit_port()), while the pending event may hold a stale pointer, eventually leading to a UAF at a later dispatch. Fortunately, there is already a refcounting mechanism (snd_use_lock_t) for the OSS MIDI device access, and for addressing the issue above, we just need to extend the refcount until the event gets dispatched. This patch extends snd_seq_oss_process_event() to give back the refcount object, which is in turn released after calling the sequencer dispatcher with the given event in the caller side. According to the original report, KASAN report as below: KASAN slab-use-after-free in snd_seq_event_dup+0x40c/0x470 RIP: 0033:0x7f2cb66a6340 Read of size 6 Call trace: dump_stack_lvl+0x73/0xb0 (?:?) print_report+0xd1/0x650 (?:?) srso_alias_return_thunk+0x5/0xfbef5 (?:?) __virt_addr_valid+0x1a7/0x340 (?:?) kasan_complete_mode_report_info+0x64/0x200 (?:?) kasan_report+0xf7/0x130 (?:?) snd_seq_event_dup+0x40c/0x470 (?:?) kasan_check_range+0x10c/0x1c0 (?:?) __asan_memcpy+0x27/0x70 (?:?) snd_seq_event_dup+0x9/0x470 (?:?) snd_seq_client_enqueue_event+0x139/0x240 (?:?) _raw_spin_unlock_irqrestore+0x4b/0x60 (?:?) snd_seq_kernel_client_enqueue+0x102/0x120 (?:?) snd_seq_oss_write+0x416/0x4e0 (?:?) apparmor_file_permission+0x20/0x30 (?:?) odev_write+0x3b/0x60 (?:?) vfs_write+0x1ce/0x850 (?:?) lock_release+0xc8/0x2a0 (?:?) __kasan_check_write+0x18/0x20 (?:?) __mutex_unlock_slowpath+0x129/0x510 (?:?) ksys_write+0xe1/0x180 (?:?) mutex_unlock+0x16/0x20 (?:?) odev_ioctl+0x65/0xc0 (?:?) __x64_sys_write+0x46/0x60 (?:?) x64_sys_call+0x7d/0x20d0 (?:?) do_syscall_64+0xc1/0x360 (arch/x86/entry/syscall_64.c:87) entry_SYSCALL_64_after_hwframe+0x77/0x7f (?:?)	2026-08-15	7.8	CVE-2026-74388
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/irdma: Fix out-of-bounds write in irdma_copy_user_pgaddrs The irdma_copy_user_pgaddrs function loops through all of the umem DMA blocks to populate the PBLs and will stop when either the last DMA block is reached or palloc->total_cnt is reached. The issue is that the logic for checking palloc->total_cnt would only work for non-zero values. When irdma_setup_pbls is called with lvl==0, it calls irdma_copy_user_pgaddrs with palloc->total_cnt==0, which means the only way to break out of the loop is to reach the last umem DMA block, which means it could end up going beyond the fixed size of 4 iwmmr->pgaddrmem array that is used in the lvl==0 case. In the case of QP/CQ/SRQ rings, the value of lvl is determined by a separate input (for example, req.cq_pages in the case of a CQ). So, we must	2026-08-15	7.8	CVE-2026-74390

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	perform explicit checking to ensure we don't overflow the pgaddrmem array if the user provides a umem that consists of more blocks than their provided req.cq_pages.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix UMR XLT cleanup on ODP populate failure mlx5r_umr_update_xlt() allocates and DMA maps an XLT buffer with mlx5r_umr_create_xlt(). The buffer is released by the common cleanup path through mlx5r_umr_unmap_free_xlt(). After mlx5_odp_populate_xlt() became fallible, its error path returned directly and skipped that cleanup. This leaks the XLT DMA mapping and buffer. If the emergency XLT page was used, it also leaves xlt_emergency_page_mutex locked. Break out of the loop so execution falls through the existing cleanup path.	2026-08-15	7.5	CVE-2026-74396
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: IB/mlx5: Fix transport-domain rollback and initialize lb mutex earlier mlx5_ib_alloc_transport_domain() allocates a transport domain and then may fail in mlx5_ib_enable_lb(). In that case, the allocated TD is leaked. Fix this by deallocating the TD when mlx5_ib_enable_lb() returns an error. Also return 0 explicitly in the no-loopback-capability success branch, and move dev->lb.mutex initialization to mlx5_ib_stage_init_init().	2026-08-15	7.8	CVE-2026-74397
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - Check for page allocation failure correctly in TIO Sashiko notes: > if __snp_alloc_firmware_pages() returns NULL under memory pressure, is it > safe to pass it directly to page_address()? > > On architectures without HASHED_PAGE_VIRTUAL, page_address(NULL) might > compute a deterministic but invalid, non-zero virtual address. The > subsequent if (tio_status) check would then evaluate to true, and > sev_tsm_init_locked() would dereference the invalid pointer. Indeed, page_address(NULL) will return non-NULL garbage here. Fix this by checking the page allocation itself for NULL, not the resulting virtual address.	2026-08-15	7.8	CVE-2026-74403
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - Fix snp_filter_reserved_mem_regions() off-by-one Sashiko notes: > regarding the bounds check in snp_filter_reserved_mem_regions() > called via walk_iomem_res_desc(): does the check > if ((range_list->num_elements * 16 + 8) > PAGE_SIZE) > allow an off-by-one heap buffer overflow? > > If range_list->num_elements is 255, 255 * 16 + 8 = 4088, which is <= 4096. > Writing range->base (8 bytes) fills 4088-4095, but writing range->page_count > (4 bytes) would write to 4096-4099, overflowing the kzalloc-allocated > PAGE_SIZE buffer. Fix this by accounting for the entry about to be written to, in addition to the entries that are already allocated.	2026-08-15	7.8	CVE-2026-74404
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: OPP: Fix race between OPP addition and lookup A race exists between dev_pm_opp_add_dynamic() and dev_pm_opp_find_freq_exact(): CPU0 (add) CPU1 (lookup) ----- _opp_add() mutex_lock() list_add(&new_opp->node, head) mutex_unlock() _opp_table_find_key() mutex_lock() dev_pm_opp_get(opp) kref_get() mutex_unlock() kref_init(&new_opp->kref) dev_pm_opp_put() kref_put_mutex() The newly added OPP is inserted into the list before its kref is initialized. A concurrent lookup can find this OPP and increment its reference count while it is still uninitialized, leading to refcount corruption and a potential premature free. Fix this by initializing ->kref and ->opp_table before making the OPP visible via list_add(). This ensures any concurrent lookup observes a fully initialized object. [Viresh: Updated commit log]	2026-08-15	7.8	CVE-2026-74405
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/radeon: fix integer overflow in radeon_align_pitch() radeon_align_pitch() has the same kind of overflow issue as the old amdgpu helper: both the alignment round-up add and the final 'aligned * cpp' calculation can overflow signed int. If that wraps, radeon_mode_dumb_create() can end up returning an invalid pitch or creating a zero-sized dumb buffer. Fix this by using check_add_overflow() for the alignment round-up and check_mul_overflow() for the final pitch calculation, returning 0 on overflow. Also reject zero pitch and size in radeon_mode_dumb_create(). Found via AST-based call-graph analysis using sqry.	2026-08-15	7.8	CVE-2026-74417
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Adjust size for copy_to_user() The amount of data returned to user space should be limited by the buffer size provided by the application. If the buffer is smaller than the data size, return only the portion that fits instead of failing.	2026-08-15	7.3	CVE-2026-74419

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: handle CB.InitCallBackState3 requests without a server record The cache manager callback path now attaches the server record to an incoming call through the rxrpc peer's app data. That association is not guaranteed to exist for every callback request, and most callback handlers already tolerate that case. Make CB.InitCallBackState3 follow the same pattern by checking whether a server record was attached before using it. If the peer is not mapped to a server record, trace the request and ignore it, matching the existing behaviour for other unmatched callback requests. This keeps the callback handler consistent with the rest of the cache manager service and avoids depending on peer state that may not be available for a given request.	2026-08-15	7.5	CVE-2026-74425
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix the reception of a reply packet before data transmission Fix rxrpc_receiving_reply() to handle the reception of an apparent reply DATA packet before rxrpc has had a chance to send any request DATA packets on a client call by checking to see if the call has been exposed yet by sending the first packet. Without this, rxrpc_rotate_tx_window() might oops. Also fix rxrpc_rotate_tx_window() to handle the Tx queue being empty by changing the do...while loop into a while loop, just in case a call is abnormally terminated by an early reply before the last request packet is transmitted.	2026-08-15	7.5	CVE-2026-74429
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix ACKALL packet handling rxrpc_input_ackall() accepts ACKALL packets without checking whether the call is in a state that can legitimately have outstanding transmit buffers. A forged ACKALL can therefore reach a new service call in RXRPC_CALL_SERVER_RECV_REQUEST before any reply packets have been queued. In that state call->tx_top is zero and call->tx_queue is NULL, so rxrpc_rotate_tx_window() dereferences a NULL txqueue and triggers a null-pointer dereference. Fix the handling of ACKALL packets by the following means: (1) Add two new call states: RXRPC_CALL_CLIENT_PRE_SEND which indicates that the client call is connected, but nothing has been transmitted as yet; and RXRPC_CALL_CLIENT_AWAIT_ACK, which indicates that everything has been transmitted at least once, but we're now waiting for the stuff remaining in the Tx buffer to be ACK'd (retransmissions may still happen). The RXRPC_CALL_CLIENT_PRE_SEND state is set when the call is assigned a channel and transitions to RXRPC_CALL_CLIENT_SEND_REQUEST when the first packet is transmitted. RXRPC_CALL_CLIENT_AWAIT_REPLY is then narrowed in scope to indicate that all Tx packets have been ACK'd and we're now waiting for the reply to be received. (2) As per Wyatt Feng's original patch[1], the ACKALL handler then checks that the call state is one in which there might be stuff in the Tx buffer to ACK, but now this includes AWAIT_ACK rather than AWAIT_REPLY. ACKALL packets are ignored if received in the wrong state. Note that unlike Wyatt Feng's patch, it's no longer necessary to check to see if the Tx buffer exists as this the state set now covers this. (3) Make the ACKALL handler use call->tx_transmitted rather than call->tx_top as the former is explicitly the highest packet seq number transmitted, whereas the latter has a looser definition. Thanks to Jeffrey Altman for a description of the history of the ACKALL packet[1].	2026-08-15	7.5	CVE-2026-74430
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix potential infinite loop in rxrpc_recvmmsg() Fix the wait in rxrpc_recvmmsg() also take check the oob queue.	2026-08-15	7.5	CVE-2026-74431
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: rxrpc_verify_data ensure rx_dec_buffer alloc rxrpc_recvmmsg_data() calls rxrpc_verify_data() whenever the rxrpc_call.rx_dec_buffer is unallocated and assumes that upon successful return that rx_dec_buffer must be allocated. However, rxrpc_verify_data() does not request an allocation if the rxrpc_skb_priv.len is zero. In addition, failure to allocate rx_dec_buffer will result in a call to skb_copy_bits() with a NULL destination which can trigger a NULL pointer dereference. To prevent these issues rxrpc_verify_data() is modified to always attempt to allocate the rxrpc_call.rx_dec_buffer if it is NULL. This issue was identified with assistance of a private sashiko instance.	2026-08-15	7.5	CVE-2026-74435
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: sun4i-ss - Remove insecure and unused rng_alg Remove sun4i_ss_rng, as it is insecure and unused: - It has multiple vulnerabilities. sun4i_ss_prng_seed() is missing locking and has a buffer overflow. sun4i_ss_prng_generate() fails to fill the entire buffer with cryptographic random bytes, because it rounds the destination length down and also doesn't actually wait for the hardware to be ready before pulling bytes from it. - No user of this code is known. It's usable only theoretically via the "rng"	2026-08-15	7.8	CVE-2026-74438

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	algorithm type of AF_ALG. But userspace actually just uses the actual Linux RNG (/dev/random etc) instead. And rng_algs don't contribute entropy to the actual Linux RNG either. (This may have been confused with hwrng, which does contribute entropy.) The sun4i_ss_prng_seed() buffer overflow was reported by Tianchu Chen and discovered by Atuin - Automated Vulnerability Discovery Engine There's no point in fixing all these vulnerabilities individually when this is unused code, so let's just remove it.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Wait on external BO kernel fences in exec IOCTL Before arming a user job, xe_exec_ioctl() only added the VM's dma-resv KERNEL slot as a dependency. That slot covers rebinds and the kernel operations of the VM's private BOs, but not external BOs (bo->vm == NULL), which carry their kernel operations (evictions, moves, ...) in their own dma-resv KERNEL slot. The DMA_RESV_USAGE_KERNEL slot is the cross-driver contract for memory management operations that must complete before the BO or its backing store may be used: any accessor is required to wait on the KERNEL fences before touching the resv. By skipping the external BOs' KERNEL slots, the exec path violated that contract and could schedule a user job while a kernel operation on an external BO mapped by the VM was still in flight, racing against it and potentially reading or writing memory that was being moved. Replace the VM-only dependency with an iteration over every object locked by the exec, adding each object's KERNEL slot as a job dependency. This covers the VM resv (rebinds and private BOs) as well as every external BO, mirroring the drm_gpuvm_resv_add_fence() call that later publishes the job fence to the same set of objects. Long-running mode continues to skip this, as before. (cherry picked from commit a6b842acf3ddd1efc53a56de9260cfa718fb35e7)	2026-08-15	7.8	CVE-2026-74440
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: validate DRAW_PRIMITIVES header size before division vmw_cmd_draw() computes maxnum = (header->size - sizeof(cmd->body)) / sizeof(*decl); where header->size is u32 and is taken straight from the user-supplied command stream. When header->size is less than sizeof(cmd->body) the unsigned subtraction wraps to nearly 4 GiB, producing a huge maxnum. Any user-controlled cmd->body.numVertexDecls then passes the bound and the loop dereferences decl[i] far past the end of the kernel command bounce buffer, producing an out-of-bounds read of kernel memory. Reject undersized headers up front.	2026-08-15	7.8	CVE-2026-74444
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: hold event_mutex while checkpointing CRIU events kfd_criu_checkpoint_events() counts the entries in p->event_idr via kfd_get_num_events(), allocates an array sized to that count, and then walks the same IDR to fill it. Neither the count nor the walk holds p->event_mutex. The CRIU checkpoint caller holds only p->mutex. Event create and destroy (kfd_event_create()/kfd_event_destroy()) take p->event_mutex and do not take p->mutex, so a second thread in the same process can insert or remove events between the count and the walk. If an event is inserted, the walk iterates more entries than were counted and writes past the end of the ev_privs allocation; if an event is removed, the walk dereferences an entry that is being freed. Hold p->event_mutex across the count and the walk so both observe a consistent view of p->event_idr. The lock is released before copy_to_user(), which only touches the local buffer. The caller already holds p->mutex and the create/destroy paths never take p->mutex, so the p->mutex -> p->event_mutex order is not inverted and no deadlock is introduced. (cherry picked from commit ff57e223ab105795b05d3ef3f3c35a5a441bcbaa)	2026-08-15	7.8	CVE-2026-74446
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: fix uint32_t overflow in EOP ring buffer size alignment eop_ring_buffer_size in struct queue_properties is a u32. In kfd_queue_acquire_buffers() the expected EOP buffer size is computed as ALIGN(eop_ring_buffer_size, PAGE_SIZE); ALIGN uses sizeof(x), so the addition is done in 32-bit. A user-supplied size of 0xFFFFF001 wraps to 0, causing kfd_queue_buffer_get() to skip its exact-size check (gated on size != 0) and accept any BO mapped at the address. On GFX8/GFX9 the MQD cp_hqd_eop_control is then programmed for an 8KB EOP ring backed by a 4KB BO, so CP EOP writes can land past the buffer and fault the GPU. Cast the operand to u64 so the alignment is computed in 64-bit; the size check in kfd_queue_buffer_get() then rejects the oversized request. (cherry picked from commit ae443117b742c357bfef3a7bddabf76fcf86e9ef)	2026-08-15	7.8	CVE-2026-74447
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix divide-by-zero in calculate_mcache_setting on zero viewport If a plane reaches calculate_mcache_setting with a zero-area viewport,	2026-08-15	7.8	CVE-2026-74449

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	calculate_mcache_setting exits early with num_mcaches == 0 and mvmpeg_width/height == 0. This will cause a divide-by-zero panic and can also cause an underflow on num_mcaches. Fix this by changing calculate_mcache_setting to bool and adding guards after each calculate_mcache_row_bytes call. If num_mcaches or mvmpeg_width/height is zero, return a false. Callers will propagate the failure as a rejected mode, which prevents the panic. (cherry picked from commit 29c0f7c655f47bcbd575ff75e58480df6ec3c9da)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix pptable use-after-free amdgpu_dpm_get_pp_table() returns a pointer to a driver-owned power table after dropping adev->pm.mutex. The sysfs path then copies from that pointer. A concurrent pp_table write can replace and free the allocation during the copy, causing a use-after-free. Change the DPM interface to copy into caller-provided storage while the mutex is held. Keep the size-only query for attribute discovery without exposing the driver-owned pointer. (cherry picked from commit f6eed7acfd30099ef7baeb6ba45bb59daad80631)	2026-08-15	7.8	CVE-2026-74450
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: validate firmware interface structure sizes iface_fw_to_cpu_addr() only checks that the firmware-provided MCU virtual address points inside the shared section. The returned pointer is later used as a full firmware interface structure, so accepting an address near the end of the shared section can still lead to out-of-bounds accesses. Pass the expected object size to iface_fw_to_cpu_addr() and reject ranges that do not fit entirely in the shared section.	2026-08-15	7.8	CVE-2026-74451
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: reject firmware sections with oversized data In panthor_fw_load_section_entry(), the data size to copy is calculated without validating it against the allocated section_size: section->data.size = hdr.data.end - hdr.data.start; If a crafted firmware sets data.size larger than the allocated memory, this could cause a heap buffer overflow in panthor_fw_init_section_mem() memcpy(section->mem->kmap, section->data.buf, section->data.size); Additionally, if the section->data.size exceeds the BO size, could this memset underflow the size calculation, leading to a massive out-of-bounds zeroing of kernel memory? memset(section->mem->kmap + section->data.size, 0, panthor_kernel_bo_size(section->mem) - section->data.size); Reject section entries whose initial data is larger than the section size.	2026-08-15	7.8	CVE-2026-74452
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: Zero the tile state data array before each BIN job The binner BO is a single 16MB buffer split into 512KB slots that are handed out to jobs at submission time and recycled as jobs complete, without ever being cleared. Each slot holds the job's Tile State Data Array (TSDA) at its start, followed by the tile allocation pool. While the tile allocation pool is only walked by the render thread through branches the binner generated during the current job, the TSDA is the PTB's own per-tile bookkeeping and is consumed by the hardware itself. Although the kernel sets the "Auto-initialise Tile State Data Array" flag in the tile binning mode configuration, the PTB demonstrably still acts on stale tile state left by the slot's previous user: the binner ends up creating invalid command streams with invalid primitive streams and branches, which can cause GPU hangs as observed in [1][2]. Zero the TSDA when the job's binning slot is configured. This clears 48 bytes per tile (~24KB for a 1080p frame) in the submission pool, and guarantees the PTB never sees another job's tile state. The tile count is only checked for being non-zero today, so the 8-bit fields it comes from can describe a tile state array almost six times larger than the slot it has to live in. Bound it before the slot is handed out, since such size decides how much of the slot is left for the tile alloc pool.	2026-08-15	7.8	CVE-2026-74453
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/vc4: Supply the overflow slot size in BPOS, not the whole bin BO size vc4_overflow_mem_work() points BPOA at a 512KB slot inside the 16MB binner BO, but writes the size of the whole BO to BPOS. On every binner out-of-memory event the PTB is therefore authorized to write tile lists across all the other slots (which may hold the tile state, tile alloc and overflow memory of in-flight jobs) and, for any slot but the first, past the end of the binner BO into unrelated CMA memory. Since CMA pages are recycled into page cache and user allocations, this is arbitrary memory corruption by GPU DMA. In practice it shows up as GPU hangs with corrupted control list pointers, userspace heap corruption, a GPU that stays permanently wedged after the first hang, and occasional full system crashes, whenever a job overflows the initial binner slot. The bug dates back to the	2026-08-15	7.8	CVE-2026-74454

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	conversion from a dedicated overflow BO (where writing the full BO size was correct) to the slotted binner BO.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: peak_usb: peak_usb_start(): fix double free of transfer buffer on URB submit error In peak_usb_start(), each RX URB transfer buffer is allocated with kmalloc() and the URB is flagged URB_FREE_BUFFER so that the final usb_free_urb() also frees the transfer buffer. If usb_submit_urb() fails, the error path frees the buffer explicitly with kfree(buf) and then calls usb_free_urb(urb). Because URB_FREE_BUFFER is set, usb_free_urb() -> urb_destroy() frees the same buffer a second time, a double free of the transfer buffer. BUG: KASAN: double-free in usb_free_urb.part.0+0x91/0xb0 Free of addr ffff8881069ccb80 by task trigger.sh/285 Call Trace: kfree+0x113/0x3c0 usb_free_urb.part.0+0x91/0xb0 Drop the redundant kfree(buf); usb_free_urb() already releases the transfer buffer. This mirrors commit 03819abbeb11 ("net: usb: lan78xx: Fix double free issue with interrupt buffer allocation").	2026-08-15	7.8	CVE-2026-74456
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: fix potential UAF on meter attach failure While attaching a newly created meter attach_meter() function makes the new meter visible to other CPUs but can still fail afterwards. On failure, it detaches the meter back and returns an error. However, this is an unexpected behavior for the ovs_meter_cmd_set() that uses a plain kfree(meter) on attach failure without waiting for RCU readers to stop using it, assuming it was never visible. This is never a problem for ovs-vswitchd as it always creates meters before creating any flows that use them. But the UAF can be triggered with a custom application using uAPI: BUG: KASAN: slab-use-after-free in ovs_meter_execute (net/openvswitch/meter.c:653) Read of size 8 at addr ffff88810d152650 by task meter/2508 Call Trace: ovs_meter_execute (net/openvswitch/meter.c:653) do_execute_actions (net/openvswitch/actions.c:1407) ovs_execute_actions (net/openvswitch/actions.c:1584) ovs_packet_cmd_execute (net/openvswitch/datapath.c:703) ... netlink_sendmsg (af_netlink.c:1900) Allocated by task 2519: __kasan_kmalloc (mm/kasan/common.c:398 mm/kasan/common.c:415) ovs_meter_cmd_set (net/openvswitch/meter.c:422) ... netlink_sendmsg (af_netlink.c:1900) Freed by task 2519: kfree (mm/slab.c:2705 mm/slab.c:6405 mm/slab.c:6720) ovs_meter_cmd_set (net/openvswitch/meter.c:479) ... netlink_sendmsg (af_netlink.c:1900) Fix that by making sure attach_meter() doesn't make the meter visible until all the checks are done and the function can't fail anymore. This also makes sure the "hash" value is calculated after the potential re-sizing of the table. Reported by Trend Micro's Zero Day Initiative as ZDI-CAN-31642.	2026-08-15	7.8	CVE-2026-74465
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/qeth: Check CAP_NET_ADMIN for private ioctls Gate the SIOCDEVPRIVATE ioctl commands SIOC_QETH_ADAP_SET_SNMP_CONTROL, SIOC_QETH_GET_CARD_TYPE and SIOC_QETH_QUERY_OAT with CAP_NET_ADMIN capable check to ensure unprivileged users cannot invoke them.	2026-08-15	7.8	CVE-2026-74467
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: scsi_debug: Fix REPORT ZONES alloc_len underflow OOB write resp_report_zones() sizes the reply buffer from the CDB allocation length. The v3 fix rounds alloc_len up with ALIGN() before deriving the descriptor count: rep_max_zones = (ALIGN((u64)alloc_len, RZONES_DESC_HD) - RZONES_DESC_HD) >> ilog2(RZONES_DESC_HD); arr_len = (u64)RZONES_DESC_HD * (rep_max_zones + 1); For alloc_len in 0xFFFFFC1..0xFFFFFFFF, ALIGN() rounds up to 0x100000000, so arr_len is 4 GB. On 32-bit, kzalloc()'s size_t is 32-bit and truncates 0x100000000 to 0; kzalloc(0) returns ZERO_SIZE_PTR, which passes the !arr check, and desc = arr + 64 is then dereferenced in the loop -> out-of-bounds write / panic. Clamp rep_max_zones to devip->nr_zones. The loop already stops at sdebug_capacity (after nr_zones zones), so a report can never hold more than nr_zones descriptors; the clamp does not change the report, it only bounds arr_len to (nr_zones + 1) * RZONES_DESC_HD, a real device property that can never reach 0x100000000.	2026-08-15	7.8	CVE-2026-74470
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tracing: Check return value of __register_event() in trace_module_add_events() trace_module_add_events() ignores the return value of __register_event() and unconditionally calls __add_event_to_tracers() for each event. If __register_event() fails (for example, if event_init() fails), the trace_event_call is not added to ftrace_events list, but __add_event_to_tracers() still creates a trace_event_file pointing to it. If module loading subsequently fails and module	2026-08-15	7.8	CVE-2026-74471

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory is freed, tracing state retains a stale trace_event_call pointer in trace_event_file, leading to a use-after-free when tracefs or tracing subsystem operations are later executed. Fix this by checking the return value of __register_event() and only calling __add_event_to_tracers() if event registration succeeded.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: pktgen: fix proc entry use-after-free pktgen_change_name() replaces pkt_dev->entry while holding t->if_lock. pktgen_remove_device() removes the same entry before __rem_dev_from_if_list() takes that lock. This allows the following interleaving: CPU 0 (NETDEV_CHANGENAME) CPU 1 (kpktgend) if_lock(t) proc_remove(pkt_dev->entry) proc_remove(pkt_dev->entry) pkt_dev->entry = proc_create_data(...) if_unlock(t) The kthread can pass the stale proc_dir_entry to proc_remove() after the rename path has freed it. A reproducer with a widened race window reports: BUG: KASAN: slab-use-after-free in proc_remove+0x78/0x80 Read of size 8 at addr ffff8881478fea70 by task kpktgend_0/67 Call Trace: proc_remove+0x78/0x80 pktgen_remove_device.isra.0+0x11c/0x4c0 pktgen_thread_worker+0x1214/0x6bc0 kthread+0x2c6/0x3b0 Allocated by task 95: __proc_create+0x204/0x790 proc_create_data+0x72/0xe0 pktgen_thread_write+0xd61/0x1510 Freed by task 28: kmem_cache_free+0xcb/0x3d0 proc_free_inode+0x5b/0x80 rcu_core+0x50a/0x1850 The buggy address belongs to the object at ffff8881478fea00 which belongs to the cache proc_dir_entry of size 192 Move proc_remove() into the if_lock-protected list removal helper. Keep it before list_del_rcu() to preserve the ordering required by add_device(). The rename path must then finish replacing the entry before removal, or it observes that the device is no longer on the list.	2026-08-15	7.8	CVE-2026-74479
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/page_reporting: use system_freezable_wq to fix UAF during suspend During PM freeze (e.g. S3 suspend or S4 hibernation), device drivers like virtio_balloon reset their underlying virtio devices and delete their virtqueues via vdev->config->del_vqs(). However, page reporting work (page_reporting_process) was scheduled on the global system_wq. Because system_wq lacks the WQ_FREEZABLE flag, the PM freezer skips it, leaving page_reporting_process active during suspend. If pages are freed into the buddy allocator while suspending (for example, when core MM invokes the balloon shrinker during S4 hibernation image saving), page reporting triggers virtballoon_free_page_report() on deleted virtqueues, resulting in a Use-After-Free / General Protection Fault: [196.795226] general protection fault, probably for non-canonical address 0xaa1436fe70dae6df: 0000 [#1] SMP NOPTI [196.825967] Workqueue: events page_reporting_process [196.831038] RIP: 0010:virtqueue_add_split+0x233/0x4c0 [virtio_ring] [196.927073] virtballoon_free_page_report+0x3a/0xe0 [virtio_balloon] [196.946943] page_reporting_process+0x370/0x4f0 Fix this by switching page reporting work to system_freezable_wq. This ensures that the PM freezer pauses page_reporting_process before device drivers destroy their reporting virtqueues. Because the reporting worker is frozen, memory reclamation/freeing (e.g. via shrinker execution) can safely return pages to MM during freeze without triggering unshrinker reporting work on deleted virtqueues. This aligns with the driver's existing design. The comment in virtballoon_freeze() states: /* * The workqueue is already frozen by the PM core before this * function is called. */ Testing: I have verified these fixes using Google's virtualization infrastructure by running continuous suspend/resume iterations (40+ cycles) while churning memory using stress-ng ('stress-ng --vm 4 --vm-bytes 60% --timeout 1') to constantly create free pages for the buddy allocator. We also set the 'page_reporting_order' parameter to 0 to make the page reporting worker highly sensitive, forcing it to pick up any 4K free pages. This confirmed that the UAF crashes are no longer reproducible.	2026-08-15	7.8	CVE-2026-74481
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: unlock i_mmap_rwsem before releasing after-split folios __folio_split() keeps dereferencing the mapping after the split: shmem_uncharge(mapping->host) and remap_page() while the folios are still frozen/locked, and i_mmap_unlock_read(mapping) at the very end, after the after-split folios have been unlocked and freed. Nothing holds an inode reference across that. The split relies on @folio -- which the beyond-EOF drop loop never removes, as it starts at folio_next(folio) -- staying locked and in the page cache to hold off eviction. But the unlock loop unlocks @folio before i_mmap_unlock_read() runs. If the caller's @lock_at is a tail beyond EOF, as memory_failure() passes when	2026-08-15	7.8	CVE-2026-74482

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	splitting a poisoned tail of a shmem THP that reaches past i_size during truncation, it too is gone from the page cache; so once @folio is unlocked no locked, in-cache folio pins the inode, and a concurrent final iput() can evict and RCU-free it before i_mmap_unlock_read() touches i_mmap_rwsem: BUG: KASAN: slab-use-after-free in __up_read+0x634/0x790 i_mmap_unlock_read include/linux/fs.h:537 [inline] __folio_split+0x732/0x1640 mm/huge_memory.c:4100 try_to_split_thp_page+0xab/0x390 mm/memory-failure.c:1675 memory_failure+0x1394/0x26e0 mm/memory-failure.c:2470 Freed by task 4601: shmem_free_in_core_inode+0x54/0xb0 mm/shmem.c:5177 evict+0x57f/0xac0 fs/inode.c:870 Do every mapping dereference while @folio still pins the inode: drop i_mmap_rwsem right after remap_page(), before the loop that unlocks and frees the after-split folios, and clear @mapping so the exit path does not unlock it again. shmem_uncharge() and remap_page() already run before that point, so after this nothing past the unlock loop touches the inode or the mapping. This is now a rule the split depends on, alongside keeping @folio frozen until the page cache is updated: no inode or mapping dereference once the after-split folios start being unlocked.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: binfmt_misc: reject a flag character as the field delimiter The registration string starts with a user chosen delimiter that separates the individual fields. So that the field parsers terminate even on a truncated string create_entry() pads the buffer with that same delimiter: memset(buf + count, del, 8); Most fields are scanned for the delimiter with strchr()/scanarg() and happily stop on the padding. The flags field is different: instead of scanning for the delimiter check_special_flags() consumes the flag characters 'P', 'O', 'C' and 'F' and stops at the first byte that is none of them, relying on the trailing delimiter to end the scan. If the delimiter is itself a flag character the padding no longer acts as a terminator. The scan swallows all eight padding bytes and keeps reading past the end of the allocation until it hits a byte that is not a flag character. For example registering PaPEPPxPPiP with 'P' as the delimiter (name "a", type extension, magic "x", interpreter "i", empty flags) leaves the flag scan running off the end of the buffer. The registration is rejected in the end because the parser does not stop exactly at buf + count, but only after the out of bounds read has already happened. With an unlucky allocation layout the scan can walk into an unmapped page; under KASAN it is reported as a slab out of bounds read. binfmt_misc mounts are available to unprivileged users in a user namespace so the read is reachable without privileges. Reject a delimiter that is one of the flag characters up front. Such a registration was always rejected anyway, only after the out of bounds read, so no valid registration string changes meaning.	2026-08-15	7.1	CVE-2026-74485
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fou: Fix use-after-free in fou_create() fou_create() publishes struct fou through sk_user_data before adding the new FOU port to the per-netns list. If fou_add_to_port_list() fails, the error path frees fou while it is still reachable through sk_user_data. A concurrent receive can then dereference the freed object in fou_from_sock(). This ordering issue was previously noted in the linked discussion. The failure is reachable when local port 0 is requested. Each socket binds to a different ephemeral port, but fou_cfg_cmp() compares the requested port 0 and reports -EALREADY once an entry already exists. Release the tunnel socket before freeing fou so sk_user_data is cleared first, and defer reclamation with kfree_rcu() to protect concurrent RCU readers. This matches the lifetime handling in fou_release().	2026-08-15	7.8	CVE-2026-74496
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: timer: Clear SNDRV_TIMER_IFLG_DEAD once the close completes snd_timer_close_locked() marks an instance with SNDRV_TIMER_IFLG_DEAD and returns early when the flag is already set, but the flag is never cleared again. A completed close ends in remove_slave_links(), which leaves timer->timer NULL, so a second close is already harmless through the timer == NULL path; the early return can only be reached by an instance that was opened again in between. For such an instance the close unlinks nothing, so snd_timer_instance_free() frees an object that is still on timer->open_list_head, still on snd_timer_master_list if it was opened with a slave key, still owns any adopted slaves, and still holds its timer and module references. snd_seq_timer_open() reopens an instance exactly like that: it retries its fallback open on the same object after a failure that has already run snd_timer_close_locked() internally. An unprivileged user with access to /dev/snd/timer and /dev/snd/seq can force that failure, since snd_timer_check_master() returns -EBUSY when a pending slave matches the new master's (slave_class, slave_id) key and the target timer has reached	2026-08-15	7.8	CVE-2026-74503

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	max_instances, and SNDRV_TIMER_IOCTL_SELECT with dev_class = SNDRV_TIMER_CLASS_SLAVE keeps the caller-supplied dev_sclass, so a sequencer queue's key can be forged. The freed instance is afterwards dereferenced by any further snd_timer_open() on that timer, by snd_timer_check_slave(), and by /proc/asound/timers, which faults on the stale ti->owner pointer. The flag only has to be visible while the close is in progress, which is all its other users need. Clear it in remove_slave_links(), under the same timer->lock that sets it, once the instance is off every list.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: afs: Fix UAF when sending a message In afs_make_call(), there's a race with async call reception and destruction. If a call is dispatched that doesn't have call->write_iter set (used to specify the data content for FS.StoreData), then the first rxrpc_kernel_send_data() will not set MSG_MORE in the msghdr. Once rxrpc_send_data() queues the last request packet, the response could come in at any time and cause the call to be completed and put. However, afs_make_call() will look at the call again to see it ->write_iter should be handled - something it's only allowed to do if it has its own ref on the call. Whilst this is the case for synchronous calls, it isn't true for async calls such as FS.FetchData. There's also a potential UAF in afs_make_call() in the event that an asynchronous call is being sent, but the call fails in some way (e.g. it gets aborted from the server). The problem there is that afs_make_call() tries to abort a call if the rxrpc send fails, but the asynchronous notification from rxrpc may have caused the afs_call to be torn down. generic/650 plays games with randomly taking CPUs offline, and can interject a significant delay such that the call is deallocated before afs_make_call() gets to check call->write_iter - and a UAF ensues (caught by KASAN). BUG: KASAN: slab-use-after-free in afs_make_call+0x1c90/0x2210 [kafs] Read of size 8 at addr ffff888035e050e8 by task fsstress/1409 Fix this by making afs_make_op_call() give the op->call its own ref rather than transferring the caller's ref to it and then dropping the ref when afs_make_call() returns. This also means that the afs_make_call() func never loses its ref on the call now.	2026-08-15	7.8	CVE-2026-74506
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: HIDP: validate numbered report payloads When hidp_get_raw_report() waits for a numbered report, hidp_process_data() compares the expected report number with skb->data[0]. A connected HIDP peer can reply with only a DATA transaction header, leaving the skb empty after the header is removed. KMSAN reports an uninitialized-value use in hidp_session_run(), with the value originating in __alloc_skb() through vhci_write(). The transaction header checks remove the empty-frame reports, but this report remains until the payload check is added. The comparison can also consume a peer-controlled byte beyond the declared L2CAP PDU. A DATA FEATURE response followed by an extra 0x01 byte made the current code accept that byte as report ID 1 and complete HIDIOCGFEATURE with a zero-byte result. With this change the malformed response is rejected with -EIO, while a subsequent valid response still succeeds. Require a payload byte before comparing a numbered report ID. Unnumbered reports continue to accept an empty payload.	2026-08-15	7.1	CVE-2026-74507
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: mgmt: fix UAF in pair command cancellation The pairing completion and authentication failure callbacks look up the pending MGMT_OP_PAIR_DEVICE command by walking hdev->mgmt_pending. The lookup returned a command that was still linked on the shared pending list, without keeping mgmt_pending_lock held for the later dereference and removal. A concurrent MGMT_OP_CANCEL_PAIR_DEVICE request can remove and free the same pending command before the callback uses it. The reverse race is also possible when cancel_pair_device() gets a command from pending_find() and a callback removes it before the cancel path dereferences it. This can lead to a use-after-free and a second list_del(). Make the pairing lookup helpers transfer ownership of the pending command by removing it from hdev->mgmt_pending while holding mgmt_pending_lock. The callbacks and cancel path then complete the command and free it directly, so racing paths cannot find or free the same command again. Take a temporary hci_conn reference in cancel_pair_device() because the command completion drops the reference stored in the pending command.	2026-08-15	7.8	CVE-2026-74510
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: mgmt: fix pending command UAF in EIR updates MGMT_OP_SET_LOCAL_NAME is handled asynchronously on powered controllers and can run set_name_sync(). When the controller is BR/EDR capable, set_name_sync() updates the local name	2026-08-15	7.8	CVE-2026-74511

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and then rebuilds EIR data through <code>eir_create()</code> . The EIR builder walks <code>hdev->uuids</code> , but the UUID list can be changed and entries can be freed by <code>MGMT_OP_ADD_UUID</code> and <code>MGMT_OP_REMOVE_UUID</code> . <code>pending_eir_or_class()</code> is meant to serialize management commands that can change EIR or the class of device, but it did not include <code>MGMT_OP_SET_LOCAL_NAME</code> . In addition, it walked <code>hdev->mgmt_pending</code> without <code>hdev->mgmt_pending_lock</code> even though pending commands are added and removed under that mutex. A racing command completion can therefore remove and free a pending command while <code>pending_eir_or_class()</code> is still inspecting it, leading to a use-after-free in the pending-command list or allowing a local name update to rebuild EIR while UUID entries are being removed. Take <code>hdev->mgmt_pending_lock</code> while scanning <code>hdev->mgmt_pending</code> and treat <code>MGMT_OP_SET_LOCAL_NAME</code> as an EIR/class-affecting pending command on the powered asynchronous path. Check for a conflicting pending command before copying the new short name so a rejected <code>SET_LOCAL_NAME</code> request does not modify <code>hdev->short_name</code> .			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: audit: fix potential use-after-free in <code>audit_del_rule()</code> <code>`audit_del_rule()'</code> destroys <code>`e->rule.exe'</code> via <code>`audit_remove_mark_rule()'</code> before unlinking the rule from RCU-visible filter lists and waiting for a grace period. Concurrent readers in <code>`audit_filter()'</code> and <code>`audit_filter_rules()'</code> still dereference <code>`e->rule.exe'</code> , while the <code>fsnotify</code> mark can be freed on an independent lifetime path. This creates a use-after-free window during rule deletion. Fix this by unlinking the rule from the RCU-visible lists and invoking <code>`synchronize_rcu()'</code> before calling <code>`audit_remove_mark_rule()'</code> (and other rule removal helpers). This ensures that all existing RCU readers have exited the critical section before any underlying resources are destroyed.	2026-08-15	7.8	CVE-2026-74512
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dmb: fix use-after-free of <code>dmb_node</code> in loopback attach/detach/unregister <code>dibs_lo_attach_dmb()</code> , <code>dibs_lo_detach_dmb()</code> and <code>dibs_lo_unregister_dmb()</code> look up the <code>dmb_node</code> under <code>dmb_ht_lock</code> , drop the lock and only then operate on the node's refcount. Nothing keeps the node alive across that window: <code>__dibs_lo_unregister_dmb()</code> removes the node from the hash table under the write lock and immediately frees it. A concurrent final put can therefore free the node between the lookup and the refcount operation: CPU0 (attach) CPU1 (owner unregisters) <code>read_lock_bh(&dmb_ht_lock)</code> find <code>dmb_node</code> (<code>refcnt == 1</code>) <code>read_unlock_bh(&dmb_ht_lock)</code> <code>refcount_dec_and_test()</code> <code>1 -> 0</code> <code>write_lock_bh(&dmb_ht_lock)</code> <code>hash_del(&dmb_node->list)</code> <code>write_unlock_bh(&dmb_ht_lock)</code> <code>kfree(dmb_node)</code> <code>refcount_inc_not_zero(&dmb_node->refcnt)</code> <-- use-after-free The same window exists for the <code>refcount_dec_and_test()</code> calls in the detach and unregister paths. Close the race structurally by making hash table membership and the refcount transitions atomic with respect to each other: - Perform the final <code>refcount_dec_and_test()</code> and <code>hash_del()</code> in a single <code>dmb_ht_lock</code> write-side critical section, in both the unregister and the detach path. Freeing the node still happens after the lock is dropped, which is safe because a node whose refcount reached zero has left the hash table and can no longer be found. - This establishes the invariant that any node found in the hash table holds at least one reference, and that the final reference can only be dropped under the write lock. <code>dibs_lo_attach_dmb()</code> can thus take its reference with a plain <code>refcount_inc()</code> while still holding the read lock; <code>refcount_inc_not_zero()</code> is no longer needed. <code>__dibs_lo_unregister_dmb()</code> no longer touches the hash table and is renamed to <code>dibs_lo_free_dmb()</code> accordingly. Note: commit <code>cc21191b584c</code> ("dibs: Move data path to dibs layer") moved the code to its current location; the race was introduced earlier by commit <code>c3a910f2380f</code> ("net/smc: implement DMB-merged operations of loopback-ism"). Tested SMC-D via ISM and dibs loopback.	2026-08-15	7.8	CVE-2026-74513
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix list corruption in <code>allocate_file_region_entries()</code> <code>allocate_file_region_entries()</code> tops up <code>resv->region_cache</code> with freshly allocated <code>file_region</code> descriptors. The allocation uses <code>GFP_KERNEL</code> , so <code>resv->lock</code> is dropped around it: the new entries are gathered on a stack-local list head, allocated <code>regions</code> , and spliced into <code>resv->region_cache</code> once the lock is re-acquired. The splice used <code>list_splice()</code> , which moves the entries but does not re-initialize the source head, so <code>allocated_regions</code> is left pointing at an entry that now lives on <code>resv->region_cache</code> . The top-up runs in a while loop that re-checks the cache deficit after re-acquiring the lock. For a shared mapping the <code>resv_map</code> is shared by every mapper of the <code>hugetlbfs</code> inode, so a concurrent <code>region_chg()/region_add()/region_del()</code> on the same <code>resv_map</code> can consume cache	2026-08-15	7.8	CVE-2026-74518

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	entries during the unlocked window and force a second iteration. That iteration calls list_add() on the stale head and corrupts the list; with CONFIG_DEBUG_LIST the __list_add_valid() check trips: list_add corruption. next->prev should be prev (ffffc900011ff7f8), but was ffff88814c281460. (next=ffff88814c545640). kernel BUG at lib/list_debug.c:31! allocate_file_region_entries+0x191/0x420 region_chg+0x267/0x300 hugetlb_reserve_pages+0x387/0xc80 hugetlbf file_mmap+0x2ce/0x3f0 mmap_region+0x1348/0x1a80 do_mmap+0x85e/0xb90 vm_mmap_pgoff+0x18c/0x330 ksys_mmap_pgoff+0x2a1/0x3e0 do_syscall_64+0xd7/0x420 Without CONFIG_DEBUG_LIST the bad list_add() silently links a kernel-stack address into resv->region_cache, leading to later use-after-free. This was observed as a real host panic on a dense KVM host where a QEMU guest-RAM hugetlbf file was mapped MAP_SHARED by both QEMU and a separate SPDK/DPDK vhost-user target, generating concurrent region_* traffic on one shared resv_map. Use list_splice_init() so the source head is re-initialized empty after each splice, making the retry loop safe.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: pinctrl: devicetree: don't free uninitialized dev_name on error path dt_remember_or_free_map() duplicates dev_name for each map entry. If kstrdup_const() fails, dt_free_map() frees dev_name in all num_maps entries, including entries that have not been initialized. Some pinctrl drivers, including pinctrl-imx, allocate the map with kmalloc() and leave dev_name for the core to initialize. The untouched entries therefore contain uninitialized data which is passed to kfree_const(). Reproduced on qemu's mcimx6ul-evk (pinctrl-imx) with failslab injection while binding the pinctrl-consuming device, under KASAN: BUG: KASAN: double-free in dt_free_map+0x34/0xa4 Free of addr c425a900 by task init/1 kfree from dt_free_map+0x34/0xa4 dt_free_map from dt_remember_or_free_map+0x184/0x198 dt_remember_or_free_map from pinctrl_dt_to_map+0x33c/0x4c8 pinctrl_dt_to_map from create_pinctrl+0x9c/0x5c0 Initialize all dev_name fields to NULL before duplicating the device name, making the full-map cleanup safe after a partial failure.	2026-08-15	7.8	CVE-2026-74519
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: qede: sync udp_tunnel ports outside qede_lock in the recovery path A TX timeout on a qede NIC that has VXLAN/GENEVE tunnel ports configured wedges the rtnetlink control plane of the whole machine: NETDEV WATCHDOG: ens6f1 (qede): transmit queue 2 timed out 10226 ms [qede_tx_timeout:586(ens6f1)]TX timeout on queue 2! [qede_recovery_handler:2665(ens6f0)]Starting a recovery process The recovery path deadlocks on the driver's own mutex: qede_sp_task rtnl_lock() mutex_lock(&dev->qede_lock) <- taken qede_recovery_handler qede_load udp_tunnel_nic_reset_ntf __udp_tunnel_nic_device_sync info->sync_table == qede_udp_tunnel_sync mutex_lock(&dev->qede_lock) <- same task: deadlock The mutex is not recursive, so the kworker blocks on itself with rtnl_lock held, and neither lock is ever released. Every task that calls rtnl_lock() afterwards (ip, ovs-vswitchd, lldpad, IPv6 addrconf, sshd) blocks forever while the node still answers ping. In a vmcore from an affected production node rtnl_mutex.owner decodes to the very kworker blocked at the innermost mutex_lock() above. Re-sync the tunnel ports from qede_sp_task() after the internal lock is dropped, still under rtnl_lock as the udp_tunnel API requires. This mirrors qede_open(), which calls udp_tunnel_nic_reset_ntf() under rtnl without the internal lock. qede_recovery_handler() now returns whether it has successfully reloaded an open device, and the caller re-syncs the ports only in that case. This keeps the old gating exactly: a device that was down or a failed recovery returns false, as those paths never reached the udp_tunnel_nic_reset_ntf() call before either. This was the only user of the qede_lock()/qede_unlock() helpers, so remove them.	2026-08-15	7.5	CVE-2026-74523
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: hold conn in hci_connect_pa_sync() callback There is theoretical UAF if the conn is freed while the hci_sync task is running. Hold refcount to avoid that.	2026-08-15	7.8	CVE-2026-74529
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_u32: validate offshift to prevent shift-out-of-bounds u32_change() copies the user-provided tc_u32_sel.offshift (unsigned char, 0-255) into the kernel knode object without bounds validation. When a packet later hits u32_classify() with TC_U32_VAROFFSET set, it evaluates `ntohs(offmask & *data) >> offshift` where the left operand is a 16-bit value promoted to a 32-bit int. Any offshift >= 32 is undefined behavior per C11 6.5.7p3, triggerable by an unprivileged user via user/network namespaces. UBSAN: shift-out-of-bounds in	2026-08-15	7.8	CVE-2026-74544

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	net/sched/cls_u32.c:236:43 shift exponent 32 is too large for 32-bit type int Fix this by rejecting offshift >= 16 during filter creation in u32_change().			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: forcedeth: fix UAF of txrx_stats in nv_remove nv_remove() frees the per-CPU txrx_stats before unregister_netdev(). Until unregister completes, ndo_get_stats64, the NAPI/xmit data path, and nv_close()/drain may still access txrx_stats, leading to a use-after-free. Free the stats only after unregister_netdev().	2026-08-15	7.8	CVE-2026-74548
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (nct6775-core) Prevent access to unsupported weight registers Sashiko reports: During initialization of the nct6116 chip, the driver sets data->pwm_num to 5. However, it assigns several NCT6106 register arrays (such as NCT6106_REG_WEIGHT_DUTY_STEP, NCT6106_REG_WEIGHT_TEMP_SEL, and NCT6106_REG_WEIGHT_TEMP_*) to data->REG_PWM and data->REG_WEIGHT_TEMP. These arrays only contain 3 elements. In nct6775_update_pwm(), the driver iterates up to data->pwm_num. If data->has_pwm has bits 3 or 4 set (which is structurally possible for nct6116), the loop attempts to read elements at index 3 and 4 from these 3-element arrays. This results in a global out-of-bounds read, which can be caught by KASAN. Furthermore, the driver uses these garbage out-of-bounds values as hardware register addresses for subsequent read and write operations. This leads to invalid hardware register access, potentially causing hardware misconfiguration or system crashes. The underlying problem is that the chip does support up to five fan control channels, but only the first three support weight control. Fix the problem by extending the affected weight register arrays with zeroed fields. The driver uses zeroed register addresses to determine if a register is supported or not, and skips accesses for unsupported registers.	2026-08-15	7.8	CVE-2026-74549
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: do not send ICMP/NDISC Redirects when peer allocation fails When inet_getpeer_v4() or inet_getpeer_v6() fails to allocate a peer entry under memory pressure or tree size caps, redirect handlers previously fell back to sending un-rate-limited ICMP/NDISC Redirect messages. In IPv4, ip_rt_send_redirect() called icmp_send() directly when peer == NULL. In IPv6, ip6_forward() and ndisc_send_redirect() passed a NULL peer into inet_peer_xrlim_allow(), which returned true when peer == NULL. Because ICMP/NDISC Redirects are not part of the default global rate limit mask (sysctl_icmp_ratemask), sending redirects when peer == NULL creates an un-rate-limited ICMP packet storm. Fix this by failing closed in ip_rt_send_redirect(), ip6_forward(), and ndisc_send_redirect() when peer is NULL.	2026-08-15	7.5	CVE-2026-74550
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (nxt-smart2) DMA-align output buffer Sashiko reports: When send_output_report() calls hid_hw_output_report(), the underlying USB HID core calls usb_interrupt_msg() which maps this buffer directly for DMA. When the DMA mapping flushes or invalidates the cacheline, it will corrupt the adjacent variables (mutex, update_interval) that were modified concurrently by the CPU. This causes memory corruption due to cacheline sharing on non-coherent CPU architectures (such as ARM or MIPS). The DMA API debugging tool (CONFIG_DMA_API_DEBUG) will trigger runtime warnings for this violation. Any operation that triggers send_output_report() (like setting a fan speed or updating the interval) causes the USB DMA mapping. On systems with non-coherent caches, this structural bug causes immediate and deterministic memory corruption. Align the output buffer to ARCH_DMA_MINALIGN to fix the problem.	2026-08-15	7.8	CVE-2026-74551
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: libiscsi: Fix stale-data leak into the SCSI sense buffer iscsi_scsi_cmd_rsp() copies the sense data of a SCSI Response from the target-supplied data segment. The segment carries a 2-byte sense length followed by the sense bytes, so it must hold 2 + senselen bytes, but the bounds check only requires datalen >= senselen: senselen = get_unaligned_be16(data); if (datalen < senselen) goto invalid_datalen; memcpy(sc->sense_buffer, data + 2, min_t(uint16_t, senselen, SCSI_SENSE_BUFFERSIZE)); A target that returns a SCSI Response whose datalen equals senselen (with senselen <= SCSI_SENSE_BUFFERSIZE) makes the memcpy() from data + 2 read up to two bytes past the received data. Those bytes are stale conn->data contents and end up in the command's sense buffer, which is returned to userspace. Account for the 2-byte sense length prefix in the check.	2026-08-15	7.5	CVE-2026-74557
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rds: tcp: hold the RCU lock across ipv6_chk_addr() in rds_tcp_laddr_check() rds_tcp_laddr_check()	2026-08-15	7.8	CVE-2026-74563

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	looks up a scoped IPv6 interface with dev_get_by_index_rcu(), drops the RCU read-side lock, and only then passes the bare struct net_device * into ipv6_chk_addr(). dev_get_by_index_rcu() only keeps the device alive within the same RCU read-side section. After rcu_read_unlock(), a concurrent RTM_DELLINK can free the net_device; ipv6_chk_addr() then dereferences the stale pointer in __ipv6_chk_addr_and_flags() (e.g. l3mdev_master_dev_rcu(dev)), reading freed memory. Keep the RCU read-side lock held across the ipv6_chk_addr() call instead of dropping it right after the lookup, so the device cannot be freed while it is in use. BUG: KASAN: slab-use-after-free in __ipv6_chk_addr_and_flags (... net/ipv6/addrconf.c:1998) Read of size 8 at addr ffff8880106ec000 by task exploit/153 Call Trace: ... kasan_report (mm/kasan/report.c:595) __ipv6_chk_addr_and_flags (... net/ipv6/addrconf.c:1998) ipv6_chk_addr (net/ipv6/addrconf.c:2031 net/ipv6/addrconf.c:1972) rds_tcp_laddr_check (net/rds/tcp.c:370) rds_bind (net/rds/bind.c:248) __sys_bind (net/socket.c:1920) __x64_sys_bind (net/socket.c:1956) do_syscall_64 (arch/x86/entry/syscall_64.c:63) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_hashlimit: validate hashtable supports XT_HASHLIMIT_RATE_MATCH The XT_HASHLIMIT_RATE_MATCH flag mode changes the semantics of the dsthash_ent structure which represents an entry in the hashtable. There is a union area which uses a different layout to express the rate match mode. Update .checkentry path to validate the XT_HASHLIMIT_RATE_MATCH mode flag is requested by two or more different rules that refer to the same hashtable. Otherwise, uninitialized access to the burst field in the union is possible. Reject the use of the XT_HASHLIMIT_RATE_MATCH mode flag if set on by revision less than 3 too.	2026-08-15	7.1	CVE-2026-74564
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: make nft_object rhhtable per table The nft_object rhhtable is global, this allows for accessing objects that are being dismantled from lookup path by other existing netns. Given the nft_obj_destroy() releases the object immediately, this might lead to use-after-free of these objects that are being released. Make the existing rhhtable per table to address this issue to deal with with the nft_rcv_nl_event() path too. Update nft_obj_lookup() to take the table as non-const, otherwise, compiler complains when passing the objname_ht to rhhtable_lookup().	2026-08-15	7.8	CVE-2026-74565
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: keys: fix out-of-bounds read in keyring_get_key_chunk() For description-level chunks keyring_get_key_chunk() advances the read pointer by level * sizeof(long) past the inline prefix but only bounds-checks the prefix, so a long enough key description is read past its kmempdup(desc, desc_len + 1) allocation. Compute the full byte offset and bounds-check the description against it before reading. The walk only reaches a description-level chunk when two keys collide through the hash, x, type and domain_tag chunks, so this is reached from an unprivileged add_key(2) with a crafted pair of same-type keys whose index hashes collide; KASAN reports a slab-out-of-bounds read.	2026-08-15	7.1	CVE-2026-74567
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix deadlock between metadata writeback and transaction commit When writing out metadata extent buffers in a zoned filesystem, btree_writetpages() holds fs_info->zoned_meta_io_lock across the whole writeback loop, including the call to btrfs_check_meta_write_pointer() -> check_bg_is_active(). For the tree-log block group, check_bg_is_active() may fail to activate the zone and fall back to btrfs_zone_finish_one_bg() to free an active zone. That path waits for the running transaction to commit while still holding zoned_meta_io_lock, but the committer needs that same lock to write out the tree extents, so the two tasks deadlock: Task A (kworker, metadata writeback) Task B (fstress, transaction commit) ----- ----- wb_workfn() btrfs_commit_transaction(T) btree_writetpages() btrfs_write_and_wait_transaction() btrfs_zoned_meta_io_lock() btrfs_write_marked_extents() btrfs_check_meta_write_pointer() btree_writetpages() check_bg_is_active() [treelog_bg] btrfs_zoned_meta_io_lock() btrfs_zone_finish_one_bg() <blocks on zoned_meta_io_lock, btrfs_zone_finish() held by Task A> do_zone_finish() btrfs_inc_block_group_ro() btrfs_wait_for_commit() <blocks waiting for commit of transaction T, done by Task B> The sibling branch in check_bg_is_active() already drops zoned_meta_io_lock around do_zone_finish() for this exact reason. Do the same in the tree-log branch:	2026-08-15	7.5	CVE-2026-74572

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	release the lock around btrfs_zone_finish_one_bg() and re-acquire it afterwards. The lock only protects fs_info->active_{meta,system}_bg, which this branch does not touch, and ctx->zoned_bg keeps a reference to the block group across the unlock, so nothing is lost while the lock is dropped. This hang occasionally reproduces with fstests generic/475 on a zoned btrfs filesystem.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dmaengine: idxd: fix fdev setup failure cleanup in idxd_cdev_open() The failed_dev_add and failed_dev_name paths drop the file-device reference while wq->wq_lock is still held. If put_device(fdev) drops the last reference, idxd_file_dev_release() runs synchronously and tries to take wq->wq_lock again, deadlocking. Those paths also fall through into the later ctx cleanup labels even though idxd_file_dev_release() owns that cleanup and frees ctx. This can make idxd_xa_pasid_remove(ctx) and kfree(ctx) operate on a freed context. Move idxd_wq_get() before file-device setup can fail, since the release callback always calls idxd_wq_put(). Then unlock wq->wq_lock before put_device(fdev) and return directly from the file-device setup failure path, leaving ctx cleanup to the release callback.	2026-08-15	7.8	CVE-2026-74574
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/slab: prevent unbounded recursion in free path with new kcalloc type Commit 280ea9c3154b ("mm/slab: avoid allocating slabobj_ext array from its own slab") avoided recursive allocation of obj_exts from kcalloc caches of the same size, by bumping the obj_exts array's allocation size whenever the array size equals the size of the object being allocated. However, as reported by Danielle Costantino and Shakeel Butt, even slabs from kcalloc caches of different sizes can form a cycle by allocating obj_exts arrays from each other [1]: What happened: a KMACCALLOC_NORMAL slab's obj_exts array (used by allocation profiling / memcg accounting) is itself kcalloc()'d from a KMACCALLOC_NORMAL cache, so the "slab holds another slab's obj_exts array" relation can form cycles. With sizeof(struct slabobj_ext) == 16 and the host's geometry: - kcalloc-512 has 64 objects/slab -> array is 64*16 == 1024 bytes, served from kcalloc-1k; - kcalloc-1k has 32 objects/slab -> array is 32*16 == 512 bytes, served from kcalloc-512. A kcalloc-512 slab and a kcalloc-1k slab therefore hold each other's obj_exts array. Discarding one frees the other's array, which empties and discards that slab, which frees the first's array, and so on: __free_slab() -> free_slab_obj_exts() -> kfree() -> discard_slab() -> __free_slab() recurses along the cycle until the stack is exhausted. With memory allocation profiling, this allows unbounded recursion in the free path and led to a stack overflow on a production host in the Meta fleet [1]: BUG: TASK stack guard page was hit Oops: stack guard page RIP: 0010:kfree+0x8/0x5d0 Call Trace: __free_slab+0x66/0xc0 kfree+0x3f0/0x5d0 ... (~125x __free_slab <-> kfree) ... <kernel driver freeing a resource> do_syscall_64 It is proposed [1] to resolve this issue by always serving the obj_exts array allocation from kcalloc caches (or large kcalloc) of sizes larger than the object size. However, as pointed out by Vlastimil Babka [2], this can waste an excessive amount of memory as slabs from large kcalloc sizes (e.g. kcalloc-8k) generally need obj_exts arrays much smaller than the object size. Therefore, rather than bumping the size, let us take a different approach; disallow formation of cycles between kcalloc types when allocating obj_exts arrays. Currently, all obj_exts arrays are served from normal kcalloc caches. Cycles cannot be created if obj_exts arrays of normal kcalloc caches are served from a special kcalloc type that can never have obj_exts arrays. To achieve this, create a new kcalloc type called KMACCALLOC_NO_OBJ_EXT. KMACCALLOC_NO_OBJ_EXT caches are created with SLAB_NO_OBJ_EXT flag when either 1) memory allocation profiling is not permanently disabled, or 2) kcalloc types with a priority higher than KMACCALLOC_CGROUP are aliased with KMACCALLOC_NORMAL. Sheaf bootstrapping for KMACCALLOC_NO_OBJ_EXT caches now must be deferred because allocation of a barn can trigger obj_exts array allocation of normal kcalloc caches when the KMACCALLOC_NO_OBJ_EXT cache for that size is not ready yet. For simplicity, perform bootstrapping of sheaves for all kcalloc caches later. Introduce a new slab alloc flag, SLAB_ALLOC_NO_OBJ_EXT, to prevent allocation of obj_exts arrays, and let kcalloc_slab() override the type to KMACCALLOC_NO_OBJ_EXT when specified. Note that kcalloc_type() remains unchanged because kcalloc_flags() bypasses the kcalloc fastpath. Do not pass SLAB_ALLOC_NO_RECURSE to kcalloc_flags() in alloc_slab_obj_exts() and instead use SLAB_ALLOC_NO_OBJ_EXT only when the objects are allocated from normal kcalloc caches. While this prevents unbounded recursive allocation of obj_exts, it allows KMACCALLOC_NO_OBJ_EXT caches to have sheaves. Since sheaf allocations specify SLAB_ALLOC_NO_RECURSE that prevents allocation of both sheaves and	2026-08-15	7.5	CVE-2026-74576

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	obj_exts arrays, the recursion depth is bounded. obj_exts arrays for non- --- truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: algif_skcipher - force synchronous processing on trees without ctx->state The AIO/async path in skcipher_recvmg() passes the socket-wide ctx->iv directly into the skcipher request. After io_submit() the socket lock is dropped and the request is processed asynchronously, so a concurrent sendmsg(ALG_SET_IV) can overwrite ctx->iv and make the in-flight request run under an attacker-controlled IV. For CTR/stream modes this is IV/keystream reuse and lets an unprivileged user recover the plaintext of a concurrent operation. Snapshotting ctx->iv into per-request storage for the async path is not sufficient. For ciphers with statesize == 0 - which includes cbc and ctr - the MSG_MORE inter-chunk IV chaining is carried solely by the in-place req->iv writeback, which a snapshot redirects into per-request memory that af_alg_free_resources() releases on completion, silently producing wrong output. Writing the IV back from the completion callback instead is not possible either: that would require lock_sock() there, but the callback can run in softirq/atomic context, so it must not sleep. Make the operation synchronous instead, which removes both the IV race and any writeback race. This is equivalent to the upstream resolution, commit fcc77d33a34c ("net: Remove support for AIO on sockets"), which removed the AIO socket path across net/ entirely and so produces the same end state for this file. This patch deviates from that commit deliberately: rather than removing AIO socket support tree-wide, which would be far too invasive for stable, it removes only the AIO branch in crypto/algif_skcipher.c. io_submit() now completes synchronously; AF_ALG async is rarely used in practice. The -EIOCBQUEUED check in skcipher_recvmg() is now dead but harmless, and is left alone to keep the fix minimal. Tested on 6.6.y: attacker IV injection dropped from 2296/200000 to 0/200000 after the change; MSG_MORE chunked CTR output bit-identical to single-shot.	2026-08-16	7.1	CVE-2026-74578
LiquidThemes--AI Hub	Subscriber Arbitrary File Download in AI Hub <= 1.3.10 versions.	2026-08-13	7.7	CVE-2026-65582
lobehub--lobe-chat	A stored cross-site scripting (XSS) vulnerability in lobehub/lobe-chat through v2.2.13 allows a low-privileged authenticated user to inject arbitrary JavaScript into the application by uploading a crafted SVG file as a user avatar.	2026-08-10	7.6	CVE-2026-72594
lucasgelfond--ZeroBrew	ZeroBrew version 0.3.1 and prior contains a missing integrity verification vulnerability in the Ruby compatibility shim that allows network attackers to execute arbitrary code by substituting malicious content at formula resource or URL-based patch URLs without checksum validation. Attackers can intercept or replace downloads for secondary resource and patch paths in shim.rb, injecting attacker-controlled build steps or source tree modifications that execute during source builds via 'zb install --build-from-source' without any integrity warning.	2026-08-14	7.5	CVE-2026-53970
magepeopleteam--Car Rental Manager	Editor PHP Object Injection in Car Rental Manager <= 1.3.9 versions.	2026-08-13	7.2	CVE-2026-27380
magepeopleteam--Taxi Booking Manager for WooCommerce	Unauthenticated Broken Access Control in Taxi Booking Manager for WooCommerce <= 2.0.3 versions.	2026-08-13	7.5	CVE-2026-27345
Mailchimp--MailChimp For WooCommerce	Administrator SQL Injection in MailChimp For WooCommerce < 6.2 versions.	2026-08-13	7.6	CVE-2026-73346
mar10--wsgidav	WsgiDAV is a generic and extendable WebDAV server based on WSGI. WsgiDAV 4.3.3 and prior can allow a WebDAV request path containing an encoded parent-directory segment to escape the configured filesystem share root in a specific path layout. The issue is fixed with version 4.3.4.	2026-08-13	7.1	CVE-2026-48099
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. Prior to 4.4.21, 4.5.14, 4.6.4, and 4.7.0-beta.1, the administrative statistics endpoints handled by Api::V1::Admin::MeasuresController and Api::V1::Admin::RetentionController checked authorization only after beginning expensive calculations. Anonymous callers could submit keys, start_at, and end_at parameters that caused long-running SQL queries in Admin::Metrics::Measure, Admin::Metrics::Retention, and Admin::Metrics::Dimension::BaseDimension, allowing repeated requests to exhaust server resources. This issue is fixed in versions 4.4.21, 4.5.14, 4.6.4, and 4.7.0-beta.1.	2026-08-10	7.5	CVE-2026-72914

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. From 4.6.0-beta.1 until 4.6.4 and 4.7.0-beta.1, any logged-in local user could use the show action in app/controllers/admin/collections_controller.rb to access personally identifying information about another local user in a collection because the controller used the general collection policy instead of the admin collection policy namespace. The exposed data included the other user's current email address and last-used IP address. This issue is fixed in versions 4.6.4 and 4.7.0-beta.1.	2026-08-10	7.5	CVE-2026-72915
matthiasnordwig--Invisible Anti-Spam & CAPTCHA Alternative for All Forms	The Invisible Anti-Spam & CAPTCHA - reCAPTCHA Alternative for All Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'action' parameter in all versions up to, and including, 5.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The stored payload is written by any unauthenticated admin-ajax.php request whose action value matches an entry in the plugin's explicit-actions list, which is auto-populated for common form builders at activation and requires no authentication gate to reach the save path.	2026-08-15	7.2	CVE-2026-16145
Metabase--Metabase	Metabase allows a remote, unauthenticated attacker to inject arbitrary SQL via the '/reset_password' database endpoint and gain administrator access to the connected Metabase instance.	2026-08-10	10	CVE-2026-72898
Metabase--Metabase	Metabase allows an unauthenticated attacker to inject arbitrary SQL via a publicly shared card or dashboard that exposes a field-filter (dimension) parameter.	2026-08-10	10	CVE-2026-72899
Microsoft--.NET 10.0	Integer overflow or wraparound in .NET allows an unauthorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-58641
Microsoft--.NET 10.0	Integer overflow or wraparound in .NET allows an unauthorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62886
Microsoft--.NET 10.0	Integer overflow or wraparound in .NET Framework allows an unauthorized attacker to execute code locally.	2026-08-11	7	CVE-2026-62897
Microsoft--.NET 10.0	Use after free in Microsoft QUIC allows an unauthorized attacker to disclose information over a network.	2026-08-11	7.5	CVE-2026-62898
Microsoft--.NET 10.0	Unchecked input for loop condition in .NET allows an unauthorized attacker to deny service over a network.	2026-08-11	7.5	CVE-2026-62901
Microsoft--.NET 10.0	Uncaught exception in .NET allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62909
Microsoft--.NET 10.0	Out-of-bounds write in .NET allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-70354
Microsoft--.NET 8.0	Out-of-bounds write in .NET allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-62871
Microsoft--App Installer	Improper privilege management in Windows Package Manager allows an authorized attacker to elevate privileges locally.	2026-08-11	7.3	CVE-2026-68821
Microsoft--Azure CycleCloud 8.9.1	Missing authorization in Azure CycleCloud allows an authorized attacker to elevate privileges over a network.	2026-08-11	8.1	CVE-2026-70340
Microsoft--Azure Kubernetes Service	Missing authentication for critical function in Microsoft Azure Kubernetes Service allows an unauthorized attacker to elevate privileges over a network.	2026-08-11	9.4	CVE-2026-50516
Microsoft--Azure Monitor Agent Linux Extension	Improper neutralization of special elements used in a command ('command injection') in Azure Monitor Agent allows an authorized attacker to elevate privileges over a network.	2026-08-11	7.2	CVE-2026-47299
Microsoft--Azure SQL Database	Incorrect permission assignment for critical resource in Azure SQL Database allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-63522
Microsoft--Azure Storage Explorer	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Storage Explorer allows an unauthorized attacker to elevate privileges over a network.	2026-08-11	8.8	CVE-2026-57104
Microsoft--Microsoft .NET Framework 3.5	Incorrect authorization in .NET Framework allows an authorized attacker to elevate privileges over a network.	2026-08-11	8.8	CVE-2026-62872
Microsoft--Microsoft .NET Framework 3.5	Relative path traversal in .NET Framework allows an unauthorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65810
Microsoft--Microsoft 365 Apps for Enterprise	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-65807

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	8.4	CVE-2026-70130
Microsoft-- Microsoft 365 Apps for Enterprise	Integer overflow or wraparound in Microsoft Office Outlook allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-70329
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-58651
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63513
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63515
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63518
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63519
Microsoft-- Microsoft 365 Apps for Enterprise	Numeric truncation error in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63525
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63526
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63527
Microsoft-- Microsoft 365 Apps for Enterprise	Integer overflow or wraparound in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63532
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-63533
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64898
Microsoft-- Microsoft 365 Apps for Enterprise	Integer overflow or wraparound in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64903
Microsoft-- Microsoft 365 Apps for Enterprise	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64904
Microsoft-- Microsoft 365 Apps for Enterprise	Buffer over-read in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64905
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Access allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64906
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64907
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Access allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64908
Microsoft-- Microsoft 365 Apps for Enterprise	Integer underflow (wrap or wraparound) in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64909
Microsoft-- Microsoft 365 Apps for Enterprise	Untrusted pointer dereference in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64910

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft 365 Apps for Enterprise	Integer overflow or wraparound in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64911
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office Access allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64912
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Access allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64914
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64915
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office Access allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64919
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Access allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-64920
Microsoft-- Microsoft 365 Apps for Enterprise	Improper neutralization of special elements used in a command ('command injection') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-65656
Microsoft-- Microsoft 365 Apps for Enterprise	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-65657
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-65661
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-65664
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-66807
Microsoft-- Microsoft 365 Apps for Enterprise	Improper neutralization of special elements used in a command ('command injection') in Microsoft Office allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-68792
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68793
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68794
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68795
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68796
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68798
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68800
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68801
Microsoft-- Microsoft 365 Apps for Enterprise	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68803
Microsoft-- Microsoft 365 Apps for Enterprise	Numeric truncation error in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68804

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68805
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds write in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68806
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68807
Microsoft-- Microsoft 365 Apps for Enterprise	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68810
Microsoft-- Microsoft 365 Apps for Enterprise	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68811
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68812
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68814
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68815
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68816
Microsoft-- Microsoft 365 Apps for Enterprise	Stack-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-68817
Microsoft-- Microsoft 365 Apps for Enterprise	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-70311
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office PowerPoint allows an unauthorized attacker to disclose information locally.	2026-08-11	7.8	CVE-2026-70313
Microsoft-- Microsoft Dynamics 365 (on-premises) version 9.1	Deserialization of untrusted data in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-65815
Microsoft-- Microsoft Edge (Chromium-based)	Heap-based buffer overflow in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-08-14	8.3	CVE-2026-72970
Microsoft-- Microsoft Entra	Insufficient verification of data authenticity in Azure Entra ID allows an authorized attacker to perform spoofing over a network.	2026-08-11	8.8	CVE-2026-62869
Microsoft-- Microsoft Entra Connect	Improper neutralization of special elements used in an sql command ('sql injection') in Microsoft Entra Connect Sync allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65673
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Authentication bypass by capture-replay in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	2026-08-11	8	CVE-2026-62911
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Heap-based buffer overflow in Microsoft Exchange Server allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62913
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Improper control of resource identifiers ('resource injection') in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	2026-08-11	7.2	CVE-2026-62910

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an authorized attacker to perform spoofing over a network.	2026-08-11	7.3	CVE-2026-62914
Microsoft-- Microsoft HPC Pack 2019	Deserialization of untrusted data in Microsoft High Performance Computing (HPC) Pack allows an unauthorized attacker to execute code over a network.	2026-08-11	9.8	CVE-2026-59124
Microsoft-- Microsoft Malware Protection Engine	Microsoft is aware of an elevation of privilege in the Microsoft Malware Protection Engine in Microsoft Defender publicly referred to as "ShieldBreak ". We are working to provide a high quality security update that addresses this vulnerability. We will provide information in this CVE when the update is available.	2026-08-14	7.8	CVE-2026-69414
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	2026-08-11	9.3	CVE-2026-70306
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper authentication in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-08-11	8.8	CVE-2026-62827
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-63514
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper input validation in Microsoft Office SharePoint allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-63520
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-64901
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Missing authentication for critical function in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-08-11	8.8	CVE-2026-64921
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-65658
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-65663
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-66805
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-66808
Microsoft-- Microsoft	Server-side request forgery (ssrf) in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-08-11	8.8	CVE-2026-70324

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SharePoint Enterprise Server 2016				
Microsoft--Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	7.3	CVE-2026-64900
Microsoft--Microsoft SharePoint Server 2019	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	8	CVE-2026-57105
Microsoft--Microsoft SharePoint Server 2019	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-65665
Microsoft--Microsoft SharePoint Server 2019	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-08-11	7.3	CVE-2026-70355
Microsoft--Microsoft SharePoint Server Subscription Edition	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-70321
Microsoft--Microsoft SharePoint Server Subscription Edition	Server-side request forgery (ssrf) in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-08-11	8.8	CVE-2026-70326
Microsoft--Microsoft Teams for Android	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Teams for Android allows an authorized attacker to perform spoofing over a network.	2026-08-11	8.8	CVE-2026-65767
Microsoft--Microsoft Teams for Android	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Teams for Android allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-65768
Microsoft--Microsoft Visual Studio Code CoPilot Chat Extension	No cwe for this issue in Visual Studio Code CoPilot Chat Extension allows an unauthorized attacker to bypass a security feature over a network.	2026-08-11	7.1	CVE-2026-65675
Microsoft--Power BI Report Server	Improper input validation in Power BI allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-65811
Microsoft--PowerShell 7.4	Relative path traversal in Microsoft PowerShell Core allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-70337
Microsoft--PowerShell 7.4	Improper neutralization of special elements used in a command ('command injection') in Microsoft PowerShell allows an authorized attacker to execute code locally.	2026-08-14	7.8	CVE-2026-50523
Microsoft--PowerShell 7.4	Server-side request forgery (ssrf) in Microsoft PowerShell Core allows an unauthorized attacker to disclose information over a network.	2026-08-11	7.4	CVE-2026-58612
Microsoft--PowerShell 7.4	Incorrect default permissions in Microsoft PowerShell allows an authorized attacker to elevate privileges locally.	2026-08-11	7.3	CVE-2026-59119
Microsoft--PowerShell 7.4	Improper control of generation of code ('code injection') in Microsoft PowerShell allows an unauthorized attacker to bypass a security feature locally.	2026-08-11	7.8	CVE-2026-70338
microsoft--prompty	Prompty is a markdown file format (.prompty) for LLM prompts. Prior to 0.1.5 and 2.0.0-beta.5, the TypeScript Nunjucks renderer evaluated untrusted .prompty template bodies with unrestricted JavaScript member access. An attacker-controlled template could traverse constructor and prototype properties to execute JavaScript in the host Node.js process. This issue is fixed in versions 0.1.5 and 2.0.0-beta.5.	2026-08-12	10	CVE-2026-73299
Microsoft--Python extension for Visual Studio Code	Inclusion of functionality from untrusted control sphere in Visual Studio Code - Python extension allows an unauthorized attacker to bypass a security feature locally.	2026-08-11	7.8	CVE-2026-54981

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft--UFO	Microsoft UFO open-source framework for intelligent automation across devices and platforms. Prior to 3.0.8, create_mobile_data_collection_server and create_mobile_action_server in ufo/client/mcp/http_servers/mobile_mcp_server.py exposed Streamable HTTP MCP services on TCP ports 8020 and 8021 without authentication, allowing an unauthenticated remote attacker to invoke capture_screenshot, get_ui_tree, tap, swipe, type_text, launch_app, press_key, and click_control against an ADB-connected Android device, disclose screen and device data, and modify device state. This issue is fixed in version 3.0.8.	2026-08-12	9.4	CVE-2026-73296
Microsoft--Visual Studio Code	Missing authorization in Visual Studio Code allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-59113
Microsoft--Visual Studio Code	Not failing securely ('failing open') in Visual Studio Code allows an unauthorized attacker to bypass a security feature over a network.	2026-08-11	8.2	CVE-2026-69306
Microsoft--Visual Studio Code	Improper neutralization of special elements used in an os command ('os command injection') in Visual Studio Code allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-69320
Microsoft--Visual Studio Code	Improper control of generation of code ('code injection') in Visual Studio Code allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-70336
Microsoft--Visual Studio Code	Authorization bypass through user-controlled key in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	2026-08-11	7.8	CVE-2026-58650
Microsoft--Visual Studio Code	Incorrect authorization in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	2026-08-11	7.8	CVE-2026-69278
Microsoft--Visual Studio Code	Improper neutralization of special elements used in an os command ('os command injection') in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-70335
Microsoft--Windows 10 Version 1607	Stack-based buffer overflow in Windows DNS allows an unauthorized attacker to execute code over a network.	2026-08-11	9.8	CVE-2026-62878
Microsoft--Windows 10 Version 1607	Use after free in Windows Deployment Services allows an unauthorized attacker to execute code over a network.	2026-08-11	9.8	CVE-2026-62893
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows iSCSI Target Service allows an unauthorized attacker to execute code over a network.	2026-08-11	9.8	CVE-2026-65791
Microsoft--Windows 10 Version 1607	Improper neutralization of special elements used in a command ('command injection') in Windows Active Directory allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-49179
Microsoft--Windows 10 Version 1607	Use after free in Windows DNS allows an unauthorized attacker to elevate privileges over a network.	2026-08-11	8.1	CVE-2026-62778
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in RPC Runtime allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-62781
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Microsoft Local Security Authority Server (lsasrv) allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62784
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows LDAP - Lightweight Directory Access Protocol allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62785
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows SMB Server allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62790
Microsoft--Windows 10 Version 1607	Stack-based buffer overflow in Windows TCP/IP allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-62792
Microsoft--Windows 10 Version 1607	Use after free in Windows LDAP - Lightweight Directory Access Protocol allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62795
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows SMB Server allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62800
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Reliable Multicast Transport Driver (RMCAST) allows an unauthorized attacker to execute code over an adjacent network.	2026-08-11	8.8	CVE-2026-62816

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Use after free in Active Directory Certificate Services (AD CS) allows an authorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62818
Microsoft--Windows 10 Version 1607	Remote Code Execution in Windows Routing and Remote Access Service (RRAS) allows attacker to gain an unauthorized access to victim's machine	2026-08-11	8.1	CVE-2026-62819
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows DNS allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-62820
Microsoft--Windows 10 Version 1607	Integer overflow or wraparound in Windows GDI+ allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62822
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows DHCP Server allows an unauthorized attacker to execute code over an adjacent network.	2026-08-11	8.8	CVE-2026-62823
Microsoft--Windows 10 Version 1607	Stack-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-08-11	8.8	CVE-2026-62824
Microsoft--Windows 10 Version 1607	Double free in Windows Secure Socket Tunneling Protocol (SSTP) allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-62889
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows iSCSI Target Service allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-65679
Microsoft--Windows 10 Version 1607	Use after free in Windows DNS allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-65789
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows iSCSI Target Service allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-65796
Microsoft--Windows 10 Version 1607	Missing authentication for critical function in Windows RPC API allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-42976
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows LUAJV allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-50472
Microsoft--Windows 10 Version 1607	Allocation of resources without limits or throttling in Windows Kernel allows an unauthorized attacker to deny service over a network.	2026-08-11	7.5	CVE-2026-54113
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Imaging Component allows an unauthorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-54984
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-59122
Microsoft--Windows 10 Version 1607	Use after free in Virtual Hard Disk (VHD) Miniport Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-59125
Microsoft--Windows 10 Version 1607	Integer overflow or wraparound in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-59127
Microsoft--Windows 10 Version 1607	Null pointer dereference in Windows TCP/IP allows an unauthorized attacker to deny service over a network.	2026-08-11	7.5	CVE-2026-59132
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-08-11	7.5	CVE-2026-59134
Microsoft--Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-61348
Microsoft--Windows 10 Version 1607	Use after free in Windows Work Folder Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61349

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-08-11	7.5	CVE-2026-61352
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61353
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-08-11	7.5	CVE-2026-61363
Microsoft--Windows 10 Version 1607	Missing authentication for critical function in Windows Remote Desktop Services allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61364
Microsoft--Windows 10 Version 1607	Missing authentication for critical function in Windows Remote Desktop Services allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61365
Microsoft--Windows 10 Version 1607	Double free in Windows Network Connection Broker allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-61366
Microsoft--Windows 10 Version 1607	Missing authentication for critical function in Windows Remote Desktop Services allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61367
Microsoft--Windows 10 Version 1607	Incorrect authorization in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61925
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows USB Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61926
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61930
Microsoft--Windows 10 Version 1607	Access of resource using incompatible type ('type confusion') in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61932
Microsoft--Windows 10 Version 1607	Integer overflow or wraparound in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61937
Microsoft--Windows 10 Version 1607	Use after free in Winlogon allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-61939
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Remote Desktop Services allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62692
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows Program Compatibility Assistant Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62696
Microsoft--Windows 10 Version 1607	Numeric truncation error in Microsoft Digest Authentication allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62698
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62700
Microsoft--Windows 10 Version 1607	Use after free in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62701
Microsoft--Windows 10 Version 1607	Use after free in Windows Modern Device Management (MDM) allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62707
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Device Association Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62710
Microsoft--Windows 10 Version 1607	Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62711

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62712
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Message Queuing allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62717
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Message Queuing allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62719
Microsoft--Windows 10 Version 1607	Insufficient granularity of access control in User-Mode Power Service (UMPS) allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62721
Microsoft--Windows 10 Version 1607	Use after free in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62723
Microsoft--Windows 10 Version 1607	Use after free in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62724
Microsoft--Windows 10 Version 1607	Use after free in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62725
Microsoft--Windows 10 Version 1607	Use after free in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62726
Microsoft--Windows 10 Version 1607	Time-of-check time-of-use (toctou) race condition in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62728
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62729
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62732
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62733
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62734
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62735
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62741
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Device Association Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62747
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62748
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Kerberos allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62752
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62753
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Kerberos allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62754
Microsoft--Windows 10 Version 1607	Stack-based buffer overflow in Windows DHCP Client allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62755

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Remote Access Connection Manager allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62758
Microsoft--Windows 10 Version 1607	Improper link resolution before file access ('link following') in Windows DHCP Server allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62761
Microsoft--Windows 10 Version 1607	Stack-based buffer overflow in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62768
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Shell allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62770
Microsoft--Windows 10 Version 1607	Use after free in Windows Kerberos allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62773
Microsoft--Windows 10 Version 1607	Use after free in Windows Graphics Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62774
Microsoft--Windows 10 Version 1607	Improper link resolution before file access ('link following') in Windows DHCP Server allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62776
Microsoft--Windows 10 Version 1607	Missing authentication for critical function in Windows License Manager allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62777
Microsoft--Windows 10 Version 1607	Use after free in Windows DNS allows an authorized attacker to execute code over a network.	2026-08-11	7.5	CVE-2026-62787
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62797
Microsoft--Windows 10 Version 1607	Improper link resolution before file access ('link following') in Windows DHCP Server allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62803
Microsoft--Windows 10 Version 1607	Improper link resolution before file access ('link following') in Windows DHCP Server allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62807
Microsoft--Windows 10 Version 1607	Improper link resolution before file access ('link following') in Windows DHCP Server allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62812
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62876
Microsoft--Windows 10 Version 1607	Stack-based buffer overflow in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62877
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62880
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62885
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows GDI+ allows an authorized attacker to execute code locally.	2026-08-11	7.8	CVE-2026-62890
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62894
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Backup Engine allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62908
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Remote Access API allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65671

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65678
Microsoft--Windows 10 Version 1607	Null pointer dereference in Windows iSCSI Target Service allows an unauthorized attacker to deny service over a network.	2026-08-11	7.5	CVE-2026-65681
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65774
Microsoft--Windows 10 Version 1607	Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65775
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65786
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65787
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Message Queuing allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65790
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Storage Port Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65814
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Key Guard allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-66799
Microsoft--Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-68820
Microsoft--Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-70307
Microsoft--Windows 10 Version 1607	Stack-based buffer overflow in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-70344
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-70345
Microsoft--Windows 10 Version 1607	Stack-based buffer overflow in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-70346
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-70347
Microsoft--Windows 10 Version 1809	Out-of-bounds write in Windows DNS allows an unauthorized attacker to execute code over an adjacent network.	2026-08-11	8.8	CVE-2026-62817
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Azure Attestation service and Device Health Attestation Service allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-66802
Microsoft--Windows 10 Version 1809	Integer overflow or wraparound in Microsoft Azure Attestation service and Device Health Attestation Service allows an unauthorized attacker to execute code over a network.	2026-08-11	8.1	CVE-2026-71331
Microsoft--Windows 10 Version 1809	Untrusted search path in Windows Narrator Braille allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-56174
Microsoft--Windows 10 Version 1809	Use after free in Windows Graphics Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-61346
Microsoft--Windows 10 Version 1809	Missing authentication for critical function in Windows Remote Desktop Services allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61356

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1809	Improper link resolution before file access ('link following') in Windows Accessibility Infrastructure (ATBroker.exe) allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61358
Microsoft--Windows 10 Version 1809	Heap-based buffer overflow in Windows Display Enhancement Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61923
Microsoft--Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62690
Microsoft--Windows 10 Version 1809	Heap-based buffer overflow in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62713
Microsoft--Windows 10 Version 1809	Heap-based buffer overflow in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62739
Microsoft--Windows 10 Version 1809	Heap-based buffer overflow in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62771
Microsoft--Windows 10 Version 1809	Heap-based buffer overflow in Windows Remote Access Connection Manager allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62783
Microsoft--Windows 10 Version 1809	Use after free in Capability Access Management Service (camsvc) allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62892
Microsoft--Windows 10 Version 1809	Improper access control in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65773
Microsoft--Windows 10 Version 21H2	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Event Logging Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-59126
Microsoft--Windows 10 Version 21H2	Heap-based buffer overflow in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61355
Microsoft--Windows 10 Version 21H2	Integer overflow or wraparound in Windows Projected File System allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62751
Microsoft--Windows 10 Version 21H2	Improper link resolution before file access ('link following') in Windows User Profile Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62832
Microsoft--Windows 10 Version 21H2	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62888
Microsoft--Windows 10 Version 22H2	Improper access control in Windows Cross Device Service allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-66804
Microsoft--Windows 11 version 23H2	Use after free in Microsoft QUIC allows an unauthorized attacker to execute code over a network.	2026-08-11	9.8	CVE-2026-62815
Microsoft--Windows 11 version 23H2	Heap-based buffer overflow in Windows Storage allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61359
Microsoft--Windows 11 version 23H2	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-61929
Microsoft--Windows 11 version 23H2	Use after free in Windows Bind Filter Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61934
Microsoft--Windows 11 version 23H2	Heap-based buffer overflow in Windows Storage allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62695
Microsoft--Windows 11 version 23H2	Heap-based buffer overflow in Windows DHCP Client allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62736

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 11 version 23H2	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62780
Microsoft--Windows 11 version 23H2	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62788
Microsoft--Windows 11 version 23H2	Heap-based buffer overflow in Windows HTTP.sys allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62811
Microsoft--Windows 11 version 23H2	Heap-based buffer overflow in Windows Remote Access API allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-65672
Microsoft--Windows 11 version 23H2	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65788
Microsoft--Windows 11 Version 24H2	Origin validation error in Windows Network Address Translation (NAT) allows an unauthorized attacker to perform spoofing over an adjacent network.	2026-08-11	8.3	CVE-2026-56179
Microsoft--Windows 11 Version 24H2	Use after free in Application Information Services allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-61357
Microsoft--Windows 11 Version 24H2	Use after free in Windows DHCP Client allows an authorized attacker to execute code locally.	2026-08-11	7	CVE-2026-61361
Microsoft--Windows 11 Version 24H2	Use after free in Windows Bind Filter Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-61927
Microsoft--Windows 11 Version 24H2	Use after free in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-61938
Microsoft--Windows 11 Version 24H2	Heap-based buffer overflow in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62688
Microsoft--Windows 11 Version 24H2	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62693
Microsoft--Windows 11 Version 24H2	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Bind Filter Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62705
Microsoft--Windows 11 Version 24H2	Heap-based buffer overflow in Windows Bind Filter Driver allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62722
Microsoft--Windows 11 Version 24H2	Untrusted pointer dereference in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62737
Microsoft--Windows 11 Version 24H2	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62749
Microsoft--Windows 11 Version 24H2	Double free in Windows Kerberos allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-62766
Microsoft--Windows 11 Version 24H2	Use after free in Windows Schannel allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62779
Microsoft--Windows 11 Version 24H2	Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65776
Microsoft--Windows 11 Version 24H2	Use after free in Windows Autopilot allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65778
Microsoft--Windows 11 Version 24H2	Use after free in Windows Autopilot allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65779

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 11 Version 24H2	Double free in Windows Autopilot allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65780
Microsoft--Windows 11 Version 24H2	Use after free in Windows Autopilot allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65781
Microsoft--Windows 11 Version 24H2	Use after free in Windows Autopilot allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65782
Microsoft--Windows 11 Version 24H2	Use after free in Windows Autopilot allows an authorized attacker to elevate privileges locally.	2026-08-11	7	CVE-2026-65783
Microsoft--Windows 11 version 26H1	Heap-based buffer overflow in Windows Container Isolation FS Filter Driver (unionfs.sys) allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62772
Microsoft--Windows 11 version 26H1	Heap-based buffer overflow in Windows SMB Client allows an authorized attacker to elevate privileges locally.	2026-08-11	7.8	CVE-2026-62799
Microsoft--Windows App Client for Windows Desktop	Execution with unnecessary privileges in Microsoft High Performance Computing (HPC) Pack allows an authorized attacker to elevate privileges over a network.	2026-08-11	8.8	CVE-2026-59133
miguelgrinberg--python-engineio	python-engineio is a Python implementation of the Engine.IO realtime client and server. Prior to version 4.13.2, an attacker can cause the creation of unnecessary background threads in the python-engineio server by exploiting the heartbeat mechanism, which launches a thread when a new connection is received, and when the client sends a PONG packet. This issue primarily affects synchronous servers. Asynchronous servers allocate background tasks instead of physical threads, which are lightweight and less likely to cause denial of service. However, the fix that was implemented was also applied to the asynchronous case. Version 4.13.2 addresses this issue as follows: The initial background thread (or async task) for heartbeat management is only launched if a client passes authentication in the 'connect' handler; and the server now ensures that there is only one background heartbeat thread (or async task) per client at a given point in time. Out of sequence PONG packets are now discarded when an active heartbeat thread is already running.	2026-08-11	7.5	CVE-2026-48802
miguelgrinberg--python-engineio	python-engineio is a Python implementation of the Engine.IO realtime client and server. Versions prior to 4.13.2 have two specific configurations of the python-engineio server in which the size of incoming messages is not checked before the messages are loaded into memory. An attacker can take advantage of these to cause unnecessary memory allocations in the python-engineio server. The two cases are POST requests, when using ASGI with the long polling transport and WebSocket messages, when using Aiohttp with the WebSocket transport. Version 4.13.2 addresses this issue. ASGI servers now only load the body of incoming requests into memory after the client is confirmed to be known and authenticated, and the payload size is below the maximum allowed size. Requests that do not comply with these requirements are discarded. Aiohttp servers configure the maximum payload size in the underlying WebSocket layer from Aiohttp, so that large messages are discarded by Aiohttp before they are delivered to python-engineio.	2026-08-11	7.5	CVE-2026-48809
miguelgrinberg--python-socketio	python-socketio is a Python implementation of the Socket.IO realtime client and server. The python-socketio server stores binary 'EVENT' and 'ACK' messages in memory while it waits to receive their binary attachments. Once all the attachments are received, these messages are then processed. Prior to version 5.16.4, an attacker can submit a binary message and intentionally omit sending one or more of its attachments to cause the message along with the partial list of received attachments to stay in memory for a long time. Version 5.16.4 takes the following measures to address this issue: Binary packets are only accepted from authenticated clients and, when a client disconnects, the server checks if there is a partial binary message being held for the client and deletes it.	2026-08-11	7.5	CVE-2026-48804
Mikado-Themes--Biagiotti Core	Unauthenticated Local File Inclusion in Biagiotti Core <= 2.1.1 versions.	2026-08-13	8.1	CVE-2026-66657
Mikado-Themes--Foton Core	Unauthenticated Local File Inclusion in Foton Core <= 1.1.1 versions.	2026-08-13	8.1	CVE-2026-66656

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MindsDB--Minds Platform	MindsDB Minds Platform version 26.1.0 and earlier contains an unauthenticated remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary OS commands by submitting crafted prompts to the unprotected POST /api/v1/responses/ endpoint, which reaches the Anton agent's scratchpad tool that calls exec() on attacker-influenced Python source without sandboxing. Attackers can first configure their own LLM API key through the unauthenticated PUT /api/v1/settings/ endpoint, then POST a prompt directing the agent to invoke the scratchpad tool with arbitrary Python code, achieving full OS command execution as the user running the desktop application and enabling access to SSH keys, stored credentials, and environment secrets.	2026-08-14	10	CVE-2026-73678
miniOrange--Headless Single Sign On	Unauthenticated Bypass Vulnerability in Headless Single Sign On <= 1.6 versions.	2026-08-13	9.8	CVE-2026-28148
miniOrange--Headless Single Sign On	Unauthenticated PHP Object Injection in Headless Single Sign On <= 1.6 versions.	2026-08-13	9.8	CVE-2026-28149
miniOrange--miniorange otp verification	Unauthenticated Privilege Escalation in miniorange otp verification <= 5.5.1 versions.	2026-08-13	9.8	CVE-2026-61967
miniOrange--OAuth Single Sign On SSO (OAuth Client)	Unauthenticated Broken Authentication in OAuth Single Sign On - SSO (OAuth Client) <= 7.0.0 versions.	2026-08-13	9.8	CVE-2026-28008
miniOrange--SAML SP Single Sign On	Unauthenticated Privilege Escalation in SAML SP Single Sign On <= 5.4.3 versions.	2026-08-13	8.1	CVE-2026-61979
minnpost--Object Sync for Salesforce	The Object Sync for Salesforce plugin is vulnerable to unauthenticated SQL Injection via the wordpress_object_type parameter of its /wp-json/object-sync-for-salesforce/push/ REST route. The route's permission callback (can_process()) checks only the HTTP method for the push class - no capability or nonce - so it is reachable by unauthenticated users. The wordpress_object_type value is concatenated directly into a SQL query (post_type = "\$object_type", class-object-sync-sf-wordpress.php:328) and executed via \$wpdb->get_results() with no \$wpdb->prepare() (:578). Because REST body parameters are not magic-quoted, an attacker can break out of the quoted string and inject arbitrary SQL. This makes it possible for unauthenticated attackers to append additional SQL queries (time-based blind), enabling extraction of sensitive information such as password hashes from the database. Only a valid wordpress_id (e.g. 1) is required - no authentication or Salesforce connection.	2026-08-15	7.5	CVE-2026-15162
Model Context Protocol--mcp-rdf-explorer	A vulnerability was detected in Model Context Protocol mcp-rdf-explorer 1.0.0. Affected is the function explore_url of the file src/mcp-rdf-explorer/server.py of the component MCP Server. Performing a manipulation of the argument url results in server-side request forgery. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-13	7.3	CVE-2026-19753
MongoDB--BI Connector ODBC Driver	The MongoDB BI Connector ODBC Driver may write outside the bounds of a fixed-size buffer when an application supplies an unusually long catalog, schema, or object name to a metadata retrieval function. This may result in memory corruption within the calling application's process, leading to abnormal termination and, under certain conditions, the potential for arbitrary code execution.	2026-08-12	9.8	CVE-2026-19001
MongoDB--BI Connector ODBC Driver	A missing bounds check when parsing stored procedure parameter metadata in the MongoDB BI Connector ODBC Driver can result in an out-of-bounds write in the client application process. Triggering this issue requires control over the server the driver connects to, or the ability to respond in its place, in order to return malformed metadata. The resulting memory corruption may cause the client application to terminate abnormally or, under certain conditions, execute unintended code.	2026-08-12	8.1	CVE-2026-19002
MongoDB--BI Connector ODBC Driver	An application using the MongoDB BI Connector ODBC Driver may experience a memory-safety issue when processing output parameters from a stored procedure. Triggering this issue requires connecting to an untrusted or impersonated database server that returns crafted metadata. This may result in process termination, disclosure of process memory, or, under certain conditions, arbitrary code execution.	2026-08-12	8.1	CVE-2026-19004

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MongoDB--BI Connector ODBC Driver	A data source definition containing an over-length file path setting may cause the MongoDB BI Connector ODBC Driver setup dialog to write outside the bounds of an allocated buffer. The issue stems from an incorrect buffer capacity calculation in the dialog's file and folder selection handling, and is reached only when a user opens the setup dialog for such a data source and initiates a file or folder selection. Depending on build configuration, the result may range from abnormal process termination to, under certain conditions, execution of unintended code in the context of the user running the dialog.	2026-08-12	7.8	CVE-2026-19003
MongoDB--MongoDB Server	An issue in MongoDB Server could allow an authenticated user with a limited database-scoped role to perform an action against protected system collections that their assigned privileges should not permit. This could result in critical system collections being dropped and recreated without proper authorization.	2026-08-11	8.1	CVE-2026-18690
MongoDB--MongoDB Server	An issue in MongoDB Server's intra-cluster connection setup could allow a party with suitable network access to influence which authentication mechanism is used when one replica set member connects to another. Under certain conditions, this could cause the cluster's shared internal credential to be transmitted in a less-protected form, potentially allowing that credential to be recovered. If recovered, the credential could be used to authenticate as the internal superuser to nodes in the deployment.	2026-08-11	8.8	CVE-2026-18691
MongoDB--MongoDB Server	An issue in MongoDB Server's handling of timeseries bucket lifecycle could allow an authenticated user with write privileges to cause an internal reference to be used after the underlying memory has been freed. Subsequent operations could then result in a server crash or, potentially, execution of unintended code.	2026-08-11	8.8	CVE-2026-18692
MongoDB--MongoDB Server	An issue in MongoDB Server's Queryable Encryption maintenance operations could allow an authenticated user with privileges on one encrypted collection to cause unauthorized modification or destruction of data belonging to a different collection. This is due to insufficient validation of certain internal metadata references before they are used to perform operations on other namespaces.	2026-08-11	8.1	CVE-2026-18712
MongoDB--MongoDB Server	MongoDB Server's handling of a Queryable Encryption maintenance operation did not properly validate certain request parameters against the collection's encrypted field configuration before use. An authenticated user with readWrite privileges could submit a specially formed request that leads to a server crash or excessive internal writes, resulting in resource exhaustion and corruption of encrypted index data.	2026-08-11	7.1	CVE-2026-18687
MongoDB--MongoDB Server	An issue in MongoDB Server's aggregation framework could allow an authenticated user to trigger an out-of-bounds memory read by providing a specially formed numeric parameter in a certain aggregation pipeline stage. This could result in a server crash (denial of service) and may potentially expose a limited amount of memory contents.	2026-08-11	7.1	CVE-2026-18688
MongoDB--MongoDB Server	An issue in MongoDB Server's handling of timeseries collections could allow an authenticated user with write privileges to cause an internal data structure to become inconsistent through certain document insertions. A subsequent insert into the affected bucket could then result in the server accessing memory outside its intended bounds, potentially causing a server crash (denial of service), exposure of limited memory contents, or memory corruption.	2026-08-11	7.6	CVE-2026-18693
MongoDB--MongoDB Server	An issue in MongoDB Server's geospatial query processing could allow an authenticated user with write privileges to cause certain malformed geometry data to be stored and later processed without proper validation. Subsequent queries against this data could then result in the server accessing memory outside its intended bounds. This could result in a server crash (denial of service) and may expose a limited amount of server process memory.	2026-08-11	7.1	CVE-2026-18694
MongoDB--MongoDB Server	An issue in MongoDB Server's aggregation framework could allow an unauthenticated party to cause a mongos (router) process to terminate unexpectedly by submitting a specially formed aggregation command. This could result in a denial of service, disrupting client connections routed through the affected mongos instance.	2026-08-11	7.5	CVE-2026-18697
MongoDB--MongoDB Server	An issue in MongoDB Server's query execution engine could allow an authenticated user with read and write privileges to cause an internal reference to be used after the underlying memory has been freed, when running certain queries against time-series collections. This could result in a server crash or disclosure of freed memory contents within query results.	2026-08-11	7.1	CVE-2026-18711
multi-parcels--MultiParcels	Unauthenticated Cross Site Scripting (XSS) in MultiParcels Shipping For WooCommerce <= 1.30.36 versions.	2026-08-13	7.1	CVE-2026-66655

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Shipping For WooCommerce				
MultiVendorX--MultiVendorX	Unauthenticated Broken Access Control in MultiVendorX <= 5.0.10 versions.	2026-08-13	7.5	CVE-2026-66441
mustafaakin--cast-localvideo	A path traversal vulnerability in mustafaakin/cast-localvideo (all versions) allows an unauthenticated remote attacker to read arbitrary files from the server. The app.js handler at lines 151-153 passes the user-supplied req.body.dir parameter directly to res.sendFile() without sanitization, enabling directory traversal via absolute paths or ../ sequences to read sensitive system files.	2026-08-10	7.5	CVE-2026-72571
MVPThemes--Reviewer	Subscriber SQL Injection in Reviewer <= 3.14.2 versions.	2026-08-13	8.5	CVE-2026-66658
Nagios Enterprises, LLC.--Nagios Core	Nagios Core before 4.5.14 and Nagios XI before 2026R1.7 contain a cross-site request forgery protection bypass via a self-supplied double-submit cookie. An attacker can supply matching cookie and request parameter values to bypass CSRF protection, enabling unauthenticated attackers to run commands as authorized users via malicious links.	2026-08-12	7.4	CVE-2026-48551
Nagios Enterprises, LLC.--Nagios Core	Nagios Core before 4.5.13 and Nagios XI before 2026R1.5 are vulnerable to authenticated remote code execution via custom-variable macro injection through the Nagios Remote Data Processor (NRDP). When a custom variable defined on a host, service, or contact is referenced in a shell-executed command line, an authenticated attacker with NRDP access can inject OS commands through the macro value. Exploitation requires a non-default configuration in which a custom variable is defined and referenced in a shell-executed command.	2026-08-12	7.5	CVE-2026-48553
Nagios Enterprises, LLC.--Nagios Core	Nagios Core before 4.5.14 and Nagios XI before 2026R1.7 are vulnerable to authenticated remote code execution via unfiltered NOTIFICATION-family macro substitution through the com_data parameter. When a notification command references \$NOTIFICATIONCOMMENT\$ or \$NOTIFICATIONAUTHOR\$ in a shell-reachable position, authenticated UI users can run arbitrary commands as the nagios user. Exploitation requires a non-default configuration in which a notification command references these macros in a shell-executed command line.	2026-08-12	7.5	CVE-2026-48554
NASA--fprime-gds	Multiple vulnerabilities in NASA fprime-gds through 3.4.3 allow an unauthenticated remote attacker to achieve arbitrary code execution on the ground station host and inject arbitrary commands to connected spacecraft. The Flask application in src/fprime_gds/flask/app.py applies no authentication to any endpoint.	2026-08-10	9.8	CVE-2026-72577
NASA--HyperCP	An OS command injection vulnerability in NASA HyperCP (main branch) allows a network-adjacent attacker who can intercept or spoof responses from oceandata.sci.gsfc.nasa.gov to execute arbitrary system commands on the researcher's workstation.	2026-08-10	7.5	CVE-2026-72579
NCEAS--metacat	Metacat is data repository software that helps researchers preserve, share, and discover data. Versions 2.x through 2.19.1 and all 1.x versions contain an unauthenticated path traversal in the `archiveEntryName` parameter of the `action=read` endpoint that is part of the original 1.x Metacat API. `ArchiveHandler.readArchiveEntry()` concatenates the user-supplied parameter into a filesystem path without validation, and the surrounding `hasReadPermission()` check is commented out. An unauthenticated remote attacker can read any file accessible to the Tomcat process by sending a single GET request. Proof-of-concept exploits have been demonstrated and verified against this vulnerability, and it should be considered easily exploitable for any Metacat deployment < 3.0.0 by any user with access to the 1.x API. Through this vulnerability, production 2.x deployments are exposed to credential theft, client certificate and private key exfiltration enabling member node impersonation within the federation, embargoed research data disclosure, and broad system reconnaissance. Given Metacat's deployment footprint across the DataONE network of repositories and federally funded research programs, the population of exposed 2.x instances is non-trivial. The vulnerability was eliminated in Metacat version 3.0.0 and after by eliminating the entire Metacat 1.x API that exposed this vulnerability. The vulnerability was remediated in April 2024 with the release of Metacat 3.0.0, which removed the legacy Metacat API including ArchiveHandler.java. The commit message and issue reference architectural cleanup, not a security fix, and no advisory or CVE was issued. The 2.x branch was not and will not be backported, as is standard practice in Metacat, which only supports the most current release. 2.19.1 remains vulnerable with identical code and is beyond its supported lifetime. As a workaround, disable or restrict 1.x API servlets. Because the vulnerable 1.x API is no longer used or necessary in most	2026-08-10	9.3	CVE-2026-47754

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Metacat deployments, restricting access to the old API endpoints can reduce or eliminate exposure for 2.19.x deployments. After removing those features, restart Tomcat or whichever software is hosting the servlets.			
NCEAS--metacat	Metacat is data repository software that helps researchers preserve, share, and discover data. Metacat versions 2.0.0 through 3.4.0 contain an unauthenticated SQL injection vulnerability in the `/cn/v1/object` and `/cn/v2/object` REST API endpoints due to unsanitized user input that can be passed through to the backend SQL database. The `nodeId` parameter can be modified to inject SQL commands, and the results are returned in error messages. Metacat appends the user-supplied data into the sql query without sanitization or parameterization. This allows extraction of arbitrary data from the underlying PostgreSQL database, fully exposing protected information to the attacker. This is accomplished by leveraging the error reporting mechanisms in Metacat, where SQL error responses are mirrored back to the caller in the XML error message returned by Metacat. One approach, for example, is to use the PostgreSQL `CAST` function to generate an error with the results of an arbitrary subquery, which is then injected into the XML error message returned by Metacat. Attackers do not need to be authenticated to execute the attack. In addition, arbitrary SQL statements that insert, update, and delete data in the Metacat database can be executed, resulting in full compromise of all data in the database. Full proof of concept attacks have been developed and verified for these vulnerabilities. The impact of this vulnerability is critical for Metacat deployments in the DataONE network where information from the database can be exfiltrated, added, changed, or deleted. This includes management information about the data catalog, access log information about who accessed data, identifying information about individuals including their ORCID identifier and client IP address, access control information about who should be able to access and modify data, and other critical internals of the data system. This sql injection vulnerability was remediated fully in Metacat version 3.4.1. If upgrading to Metacat 3.4.1 isn't immediately possible, most deployments can mitigate the issue by disabling the `/cn` REST endpoints in the webapp deployment. This API is not needed or used by member repositories in the DataONE network, as it is only used by the DataONE Coordinating Node deployments. Consequently, this API can be disabled without reduction of functionality for most deployments. To disable the vulnerable endpoints, simply remove the servlet and servlet-mapping for the `/cn` endpoints in the servlet engine associated with the two servlets, `edu.ucsb.nceas.metacat.restservice.v1.CNRestServlet` and `edu.ucsb.nceas.metacat.restservice.v2.CNRestServlet`. For example, in Tomcat, remove the relevant `servlet-mapping` elements from the application web.xml file in Metacat.	2026-08-14	9.8	CVE-2026-48528
Netatalk--netatalk	Netatalk is a Free and Open Source file server suite for Unix-like operating systems. In versions 3.1.19 through 4.4.2, a stack-based buffer overflow exists in the copydir() function of Netatalk's afpd daemon due to an integer underflow in the calculation of the remaining buffer size used for path construction. copydir() is a utility function called when a file operation crosses a device boundary inside an AFP shared volume, which the standard library's renameat() cannot handle. The function attempts to track available buffer space using srem and drem for source and destination paths. Incorrect arithmetic causes both srem and drem to underflow to SIZE_MAX. Consequently, boundary checks against strlen(de->d_name) always pass, allowing strcpy() to append filenames into nearly full stack buffers. Version 4.4.3 patches the issue. As a workaround, configure each AFP shared volume to be structured as a single file system, in other words no subdirectory of a shared volume should be a mount point for a different file system.	2026-08-14	7.5	CVE-2026-45699
Netis Systems Co., Ltd.--Netis NC63 Wireless AC1200 Router	Netis NC63 router firmware V3.0.0.3327 contains an unauthenticated firmware update vulnerability that allows unauthenticated attackers to submit unsigned firmware images by exploiting a missing authentication enforcement flaw in the Boa web server and netis.cgi CGI dispatcher. Attackers can send a multipart POST request to /cgi-bin/upload_fw.cgi without a valid session cookie, bypassing authentication because Boa grants access to any path containing '.cgi' regardless of cookie validation, and netis.cgi reads but does not enforce the authentication state before invoking the firmware update handler, which accepts images validated only by a forgeable additive checksum and static product strings rather than a cryptographic signature, potentially enabling persistent router compromise.	2026-08-14	8.8	CVE-2026-73673

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netty--netty	Netty is an asynchronous, event-driven network application framework. Prior to 4.1.136.Final and 4.2.16.Final, <code>io.netty.handler.codec.xml.XmlFrameDecoder.decode()</code> failed to preserve closing-tag parser state across invocations, so an unauthenticated remote attacker could trickle-feed repeated <code></</code> sequences that repeatedly rescanned the accumulated buffer and exhausted an EventLoop thread's CPU, causing denial of service with a <code>maxFrameLength</code> of 1 MB. This issue is fixed in versions 4.1.136.Final and 4.2.16.Final.	2026-08-13	7.5	CVE-2026-73507
nextauthjs--next-auth	NextAuth.js provides authentication for Next.js. Prior to <code>@auth/core</code> 0.41.3 and <code>next-auth</code> 4.24.15 and 5.0.0-beta.32, the exported <code>getToken()</code> helper in the <code>next-auth/jwt</code> and <code>@auth/core/jwt</code> modules can throw an uncaught exception when it reads a malformed Authorization: Bearer header. When no session cookie is present, <code>getToken()</code> URL-decodes the bearer value before validating it, and malformed percent encoding causes <code>decodeURIComponent()</code> to throw instead of treating the token as invalid. Because <code>getToken()</code> is commonly called in API routes, middleware, and server-side request handlers, a single unauthenticated request can trigger an unhandled exception in code paths that authenticate requests, causing a per-request denial of service without exposing tokens, sessions, or other data and without bypassing authentication. This issue is fixed in <code>@auth/core</code> 0.41.3 and <code>next-auth</code> 4.24.15 and 5.0.0-beta.32.	2026-08-12	7.5	CVE-2026-73418
Nishishi Factory--Tegalog -Fumy Otegaru Memo Logger-	Tegalog -Fumy Otegaru Memo Logger- provided by Nishishi Factory contains a vulnerability due to a permissive regular expression, which may allow an attacker who can access the affected product to log in to the management console. As a result, the attacker may perform any operations available from the management console.	2026-08-10	8.6	CVE-2026-64940
nodeca--js-yaml	js-yaml is a JavaScript YAML parser and dumper. From 5.0.0 until 5.2.2, parsing a small YAML document can take exponential time when an application calls <code>load()</code> or <code>loadAll()</code> on untrusted input. In <code>src/parser/parser.ts</code> , <code>readFlowCollection</code> uses <code>restoreState</code> and calls <code>parseNode</code> a second time when a flow-sequence entry is recognized as a key: value pair. If the key is a nested flow sequence of the same shape, every level is parsed twice, causing $O(2^n)$ work and allowing an input under 200 bytes to keep one CPU busy for minutes, block the Node.js event loop, and stall the process. No anchors, aliases, merges, tags, or nondefault options are required. This issue is fixed in version 5.2.2.	2026-08-13	7.5	CVE-2026-73643
o1lab--xmysql	A path traversal vulnerability in <code>o1lab/xmysql</code> (all versions) allows an unauthenticated remote attacker to read and download arbitrary files from the server. The <code>lib/xapi.js</code> file at lines 338 and 424 uses the user-controlled <code>req.query.name</code> parameter in <code>path.join(cwd, name)</code> without sanitization before passing it to <code>res.download</code> , enabling directory traversal via <code>../</code> sequences to access sensitive system files.	2026-08-10	7.5	CVE-2026-72572
Onokazu--Directories Pro	Subscriber Privilege Escalation in Directories Pro <= 2.0.5 versions.	2026-08-13	7.7	CVE-2026-66661
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.5 before 0.10.0, any authenticated user can overwrite the content of a message in a channel they do not belong to (including private and DM channels) by sending a chat completion request with a channel:-prefixed <code>chat_id</code> and a target <code>message_id</code> . The channel: path routes pipeline output through <code>_make_channel_emitter</code> , which writes to the Messages table using the caller-supplied <code>message_id</code> without binding it to the channel. This issue is fixed in version 0.10.0.	2026-08-13	7.1	CVE-2026-59714
OpenBMB--XAgent	XAgent contains a path traversal vulnerability in the workspace file endpoint that allows self-registered or default-credential users to read arbitrary files on the host by supplying parent-directory segments in the <code>'file_name'</code> form field with no path containment check. Attackers can register an account without email verification, then submit crafted <code>'file_name'</code> values such as parent-directory traversal sequences to the <code>'/workspace/file'</code> handler to read host files including application secrets, database credentials, and system files outside the Docker sandbox.	2026-08-11	7.5	CVE-2026-72713
openchoreo--backstage-plugins	OpenChoreo is a developer platform for Kubernetes. Prior to 1.0.4, 1.1.4, and 1.2.1, the OpenChoreo Backstage backend hardcoded <code>backend.auth.dangerouslyDisableDefaultAuthPolicy</code> and <code>auth.providers.guest.dangerouslyAllowOutsideDevelopment</code> to true, exposing <code>/api/*</code> without authentication and allowing unauthenticated catalog reads, scaffolder log reads, and catalog location creation or deletion. This issue is fixed in versions 1.0.4, 1.1.4, and 1.2.1.	2026-08-13	8.2	CVE-2026-73666

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openchoreo--openchoreo	OpenChoreo is a complete, open-source developer platform for Kubernetes. Prior to 1.0.3, 1.1.3, and 1.2.0-rc.2, internal/cluster-gateway/server.go exposed /api/proxy/, /api/exec/, and /api/wirelogs/ on an internal listener without requiring a client certificate or token, allowing any network-reachable caller to read tenant Kubernetes Secrets, mutate workloads, and execute commands across connected data planes. This issue is fixed in versions 1.0.3, 1.1.3, and 1.2.0-rc.2.	2026-08-13	9	CVE-2026-73842
openchoreo--openchoreo	OpenChoreo is a complete, open-source developer platform for Kubernetes. Prior to 1.0.2 and 1.1.2, internal/cluster-gateway/server.go served caller-facing management APIs on the externally reachable agent listener without authentication, allowing network-reachable attackers to invoke /api/proxy/ and /api/exec/ operations, proxy the data-plane Kubernetes API, and execute commands in workload pods in multi-cluster deployments. This issue is fixed in versions 1.0.2 and 1.1.2.	2026-08-13	9.6	CVE-2026-73843
openchoreo--openchoreo	OpenChoreo is a complete, open-source developer platform for Kubernetes. Prior to 1.0.4, 1.1.4, and 1.2.0-rc.2, OpenChoreo Workflow Plane templates under samples/getting-started/workflow-templates/ interpolated developer-controlled workflow parameters into shell program text executed through sh -c instead of passing the values through container.env, allowing arbitrary commands to run in workflow pods while affected privileged Podman templates lacked hostUsers: false. This issue is fixed in versions 1.0.4, 1.1.4, and 1.2.0-rc.2.	2026-08-13	8.8	CVE-2026-73667
openchoreo--openchoreo	OpenChoreo is a complete, open-source developer platform for Kubernetes. From 1.2.0-rc.1 until 1.2.0, internal/openchoreo-api/api/handlers/exec.go and internal/openchoreo-api/api/handlers/wirelogs.go authorize component:exec and wirelogs:view using the caller-supplied project query parameter instead of comp.Spec.Owner.ProjectName, allowing a user with a project-scoped grant to execute commands in and read wirelogs from components owned by other projects in the same namespace. This vulnerability is fixed in 1.2.0.	2026-08-13	8.8	CVE-2026-73841
OpenIdentityPlatform--OpenDJ	OpenDJ is an LDAPv3 compliant directory service. Prior to 5.1.2, the SASL PLAIN authorization identity path in opendj-server-legacy/src/main/java/org/opensds/server/extensions/PlainSASLMechanismHandler.java checked the PROXIED_AUTH privilege but did not evaluate the mayProxy proxy ACI scope when an authzid resolved to a different user. Both dn: and u: or bare authzid forms could therefore let an authenticated account holding PROXIED_AUTH assume any resolvable non-root identity outside the identities permitted by its proxy ACI. The fix returns INVALID_CREDENTIALS (49) before password verification when the target authorization identity is not permitted. This issue is fixed in version 5.1.2.	2026-08-13	9.6	CVE-2026-73644
OpenListTeam--OpenList	OpenList a file list program that supports multiple storage. Prior to 4.2.4, the authenticated /api/fs/batch_rename handler in server/handles/fsbatch.go authorizes only the source directory produced by user.JoinPath(req.SrcDir) and validates renameObject.NewName with checkRelativePath, but does not validate attacker-controlled renameObject.SrcName, supplied as src_name, before concatenating it with the authorized path and passing the result to fs.Rename. A user with rename permission can use traversal segments in src_name to make path normalization select a file outside the authorized directory and configured base path, resulting in cross-user file integrity loss, limited availability impact, and file-existence disclosure through success or error responses. This issue is fixed in version 4.2.4.	2026-08-13	7.6	CVE-2026-73509
OpenSignLabs--OpenSign	An insecure direct object reference vulnerability in OpenSignLabs OpenSign through 2.37.0 allows unauthenticated remote attackers to retrieve any contact record via the getcontact Parse cloud function. The function executes with useMasterKey and performs no authentication or authorization checks before returning the requested contact object. An attacker can enumerate and read all contact records including personally identifiable information without credentials.	2026-08-11	7.5	CVE-2026-72543
OpenSignLabs--OpenSign	An integrity verification vulnerability in OpenSignLabs OpenSign through 2.37.0 allows unauthenticated remote attackers to forge document audit-trail entries via the triggerevent Parse cloud function. The function accepts viewer identity and IP address as caller-supplied parameters without authentication, allowing fabrication of arbitrary audit log entries. An attacker can tamper with the legal audit trail of any signed document, undermining non-repudiation.	2026-08-11	7.5	CVE-2026-72544
OpenSignLabs--OpenSign	An insecure direct object reference vulnerability in OpenSignLabs OpenSign through 2.37.0 allows unauthenticated remote attackers to write to any contact record via the updatecontacttour Parse cloud function. The function performs no authentication or authorization before updating the target contact record. An	2026-08-11	7.5	CVE-2026-72545

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker can corrupt or overwrite contact data for any user in the system without credentials.			
OpenSignLabs--OpenSign	An information disclosure vulnerability in OpenSignLabs OpenSign through 2.37.0 allows unauthenticated remote attackers to retrieve any organisation tenant record via the gettenant Parse cloud function. The function accepts a contactId parameter and returns the full tenant record without authentication or authorization checks. An attacker can enumerate and disclose tenant configuration data for any organisation in the system.	2026-08-11	7.5	CVE-2026-72548
OpenSignLabs--opensignserver	A missing authentication vulnerability in OpenSignLabs opensignserver through 2.37.0 allows an unauthenticated remote attacker to read arbitrary stored documents via the fileupload Parse cloud function. The function mints MASTER_KEY-signed file access tokens for any caller-supplied URL without performing any session check, defeating the only access control protecting stored contract files.	2026-08-10	7.5	CVE-2026-72688
OpenSignLabs--opensignserver	A broken object-level authorization vulnerability in OpenSignLabs opensignserver through 2.37.0 allows an unauthenticated remote attacker to read complete contract records via the getDocument Parse cloud function. The function fetches documents using useMasterKey, bypassing the object ACL, and returns full records including sender and signer PII and a pre-signed document download URL whenever the document's IsEnableOTP flag is unset, which is the default configuration.	2026-08-10	7.5	CVE-2026-72689
OpenSignLabs--opensignserver	An authentication bypass vulnerability in OpenSignLabs opensignserver through 2.37.0 allows an unauthenticated remote attacker to mint MASTER_KEY-signed file access tokens for arbitrary stored files via the getsignedurl Parse cloud function. The function skips its isAuthenticated check whenever any docId parameter is supplied, even one corresponding to no real document, allowing the authentication gate to be bypassed by supplying an arbitrary string as docId.	2026-08-10	7.5	CVE-2026-72691
OpenSignLabs--opensignserver	A missing authorization vulnerability in OpenSignLabs opensignserver through 2.37.0 allows an unauthenticated remote attacker to irreversibly decline any in-flight document and forge the decline attribution to an arbitrary user via the declinedoc Parse cloud function. The function writes IsDeclined, DeclineReason, and a caller-supplied DeclineBy pointer without verifying the caller's identity, enabling workflow termination and evidentiary record falsification against any accessible document.	2026-08-10	7.5	CVE-2026-72692
OpenStack--Designate	In OpenStack Designate before 22.0.1, zone creation checks (_is_subzone, _is_superzone, and the duplicate-zone DB constraint) are scoped to the target pool only. An authenticated user can bypass these checks by scheduling a zone to a different pool via the AttributeFilter scheduler, creating an overlapping zone that conflicts with another tenant's zone. This enables cross-tenant DNS hijack (redirecting traffic to attacker-controlled IPs) and DNS denial of service (NODATA responses). Exploitation requires a multi-pool deployment with AttributeFilter enabled in scheduler_filters, which is a non-default but documented and supported configuration for self-service tiering.	2026-08-12	9.6	CVE-2026-71193
opentofu--opentofu	OpenTofu versions 1.8.0 through 1.8.2 do not properly restrict sensitive variables and locals when users have opted into static evaluation of module sources, versions, and backend configurations. As a result, values marked as sensitive may be exposed through these configuration elements instead of producing an error. This is fixed in OpenTofu 1.8.3, which adds explicit errors to prevent the use of sensitive values in these contexts.	2026-08-16	7.5	CVE-2024-58375
openwrt--luci	luci-app-ovpn fails to properly validate the instance_name2 parameter during file upload, allowing authenticated users to perform path traversal and write arbitrary files outside the intended directory. Attackers can upload malicious payloads to gain persistent root code execution by placing SSH keys in system directories accessible on reboot.	2026-08-13	9.9	CVE-2026-72841
openwrt--luci	luci-app-lxc contains an ACL inconsistency vulnerability that allows low-privileged authenticated LuCI users to access backend container management routes without proper authorization checks. Attackers can exploit path traversal via `/.%2E` in the `lxc_name` parameter to escape container directories and control host-side scripts executed through `lxc.hook.start-host`, achieving root code execution on the OpenWrt host.	2026-08-13	9.9	CVE-2026-72842
openwrt--luci	OpenWrt LuCI contains an overly permissive ACL definition in luci-mod-system-mounts that grants write access to /etc/crontabs/root to users intended only for mount configuration. Authenticated users with only the mount-configuration ACL	2026-08-13	8.8	CVE-2026-72840

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	group can append arbitrary cron entries via ubus file.write, which the default busybox crond daemon executes as root within one minute.			
oscal-compass--compliance-trestle	compliance-trestle is a tooling platform for managing compliance as code. Versions prior to 3.12.2 and 4.0.3 have a Server-Side Template Injection (SSTI) vulnerability exists in the `trestle author jinja` command. The command recursively evaluates rendered templates, allowing an attacker to achieve arbitrary command execution with privileges of the running process by injecting malicious payloads into data fields (such as SSP documents or Lookup Tables). The vulnerability does not require attacker control of the template itself. Only attacker-controlled input data rendered into a trusted template is required. This distinction is critical: the template author may only intend to render plain text (e.g., `Title: {{ ssp.metadata.title }}`), but because of the recursive parsing, the data field itself becomes executable. The vulnerability is caused by recursive re-compilation and re-rendering of already-rendered output. Versions 3.12.3 and 4.0.3 patch the issue.	2026-08-14	7.8	CVE-2026-46439
owen2345--CamaleonCMS	CamaleonCMS version 2.9.2 and earlier contains a privilege escalation vulnerability via insecure direct object reference (IDOR) that allows authenticated low-privileged attackers to overwrite any user's credentials by exploiting a parameter confusion flaw between the authorization filter and action body in the UsersController. Attackers can send a PATCH request to the updated_ajax endpoint setting params[:id] to their own user ID to pass the self-authorization check while simultaneously setting params[:user_id] to a victim's ID, causing the controller to load and mutate the victim's account, including overwriting administrator passwords to achieve full site takeover.	2026-08-11	8.8	CVE-2026-56721
owen2345--CamaleonCMS	CamaleonCMS contains a stored cross-site scripting vulnerability that allows authenticated low-privileged users to execute arbitrary JavaScript in an administrator's browser by injecting unsanitized HTML payloads into the post title parameter during draft creation. Attackers can submit a malicious HTML payload as a draft title through the drafts creation endpoint, which is persisted to the database without escaping and later rendered as raw HTML in the admin drafts listing, enabling administrator session compromise, cookie theft, and forged authenticated requests.	2026-08-12	8.7	CVE-2026-73329
owen2345--CamaleonCMS	CamaleonCMS contains a stored cross-site scripting vulnerability in the cama_contact_form plugin that allows low-privileged authenticated attackers to inject arbitrary HTML by submitting unsanitized content to the before_html field through the contact form edit endpoint, which lacks proper authorization controls. Attackers can persist malicious script payloads into the database that execute in victims' browsers when the contact form loads, enabling cookie theft, forged authenticated requests against the admin interface, and session takeover of viewing users.	2026-08-12	8.7	CVE-2026-73332
owen2345--CamaleonCMS	CamaleonCMS contains a missing authorization vulnerability that allows any authenticated low-privileged user to access and modify plugin settings by reaching four unprotected plugin-administration endpoints without administrator-level authorization. Attackers can manipulate plugin configuration parameters at runtime across the attack, front_cache, cama_meta_tag, and cama_contact_form plugins to alter cached page behavior, modify public meta-tag output, or reconfigure contact forms, enabling account takeover when chained with stored cross-site scripting through the contact form's before_html field.	2026-08-12	7.6	CVE-2026-73326
owen2345--CamaleonCMS	CamaleonCMS 2.9.1 contains an authenticated SQL injection vulnerability that allows authenticated attackers with post creation or editing privileges to submit a crafted slug value containing SQL syntax that the database backend evaluates as part of an inadequately parameterized query. Attackers can supply malicious slug payloads using boolean- or union-style blind SQL injection techniques to extract sensitive data from the underlying SQLite database, including administrative credentials and configuration values stored in application tables.	2026-08-12	7.1	CVE-2026-73331
paoltaia--GeoDirectory WP Business Directory Plugin and Classified Listings Directory	The GeoDirectory - WP Business Directory Plugin and Classified Listings Directory plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_revision function in all versions up to, and including, 2.8.169. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). By placing post_type=attachment exclusively in the query string to bypass the consistency check, an attacker can convert an auto-draft GeoDirectory listing into a WordPress attachment with attacker-controlled file paths injected into attachment	2026-08-11	8.1	CVE-2026-19091

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	metadata, which the delete_revision handler then dereferences and unlinks without any post-type or path validation.			
papersgpt--papersgpt-for-zotero	PapersGPT for Zotero 0.6.1 contains a remote code execution vulnerability that allows attackers to execute arbitrary JavaScript by returning malicious code from an LLM endpoint that is passed unsanitized to window.eval() in views.ts. Attackers can exploit this through prompt injection in PDFs, MITM interception of API requests, or a malicious custom LLM endpoint to execute arbitrary code in Zotero's chrome-privileged context, enabling file read/write, process execution, and access to all Zotero data.	2026-08-11	9.6	CVE-2026-73032
Peppermint Lab--Peppermint	A broken access control vulnerability in Peppermint Lab Peppermint through commit ba6e217 exists because the Config.roles_active flag defaults to false, causing all permission checks on ticket, client, and user handlers to behave as no-ops on default installations. All authenticated users bypass ownership and administrative access controls. An attacker with any user account can read, modify, or delete tickets, clients, and users belonging to any other account.	2026-08-11	8.1	CVE-2026-72555
Peppermint Lab--Peppermint	A broken access control vulnerability in Peppermint Lab Peppermint through commit ba6e217 allows any authenticated non-administrative user to reconfigure the platform global OIDC/SSO settings via an unprotected configuration endpoint. The endpoint performs no administrative role check before applying new OIDC issuer settings. An attacker can redirect all SSO logins to an attacker-controlled identity provider, enabling credential harvesting for all platform users.	2026-08-11	8.8	CVE-2026-72561
Pete Nelson--REST API Log	Unauthenticated Sensitive Data Exposure in REST API Log <= 1.7.1 versions.	2026-08-13	7.5	CVE-2026-66443
Phoenix Contact--AXC F 1152	The device's PROFINET service is affected by a buffer overflow vulnerability that exists in the default configuration. An unauthenticated remote attacker could exploit this vulnerability to reboot the device or execute arbitrary code.	2026-08-12	9.8	CVE-2025-41769
Phoenix Contact--AXC F 1152	An unauthenticated denial-of-service vulnerability in the device's PLCnext Engineer communication interface allow an remote attacker to interrupt access via the client application. Successful exploitation prevents communication until the PLCnext service is manually restarted.	2026-08-12	7.5	CVE-2025-41770
phplist--phplist3	phplist before 3.7.0-RC5 contains a cross-site request forgery (CSRF) vulnerability in lists/admin/admins.php. The administrator deletion action is triggered via an unauthenticated GET request (?page=admins&delete=N) that is not protected by a CSRF token (the central verifyCsrfGetToken check uses enforce=false and is bypassed when the token parameter is absent). A remote attacker can trick a logged-in super-administrator into loading a crafted URL (e.g., embedded as an image in an email) to delete any non-self administrator account.	2026-08-13	8.1	CVE-2026-73482
pietror91--RapiSafe Secure Multi File Upload for Contact Form 7	The RapiSafe - Secure Multi File Upload for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the handleAjaxRemoveUpload function in all versions up to, and including, 1.0.4. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The nonce required to invoke the removal handler is exposed in public-facing JavaScript as RSMFCF7Vars.nonce on every Contact Form 7 page rendering a RapiSafe upload field, making it obtainable by any unauthenticated visitor.	2026-08-15	9.1	CVE-2026-14484
pimcore--pimcore	Pimcore's Admin Classic Bundle provides a Backend UI for Pimcore. Versions prior to 2.3.6 and 1.7.18 have a SQL injection vulnerability in Pimcore's translation grid date filter - the user-supplied `property` field from the filter JSON is interpolated directly into a `UNIX_TIMESTAMP(DATE(FROM_UNIXTIME(...)))` SQL expression without parameterization or allowlist validation. Versions 2.3.6 and 1.7.18 fix the issue.	2026-08-12	8.8	CVE-2026-44741
Pimcore--pimcore admin-ui-classic-bundle	An SQL injection vulnerability in Pimcore admin-ui-classic-bundle through version 2.3 allows authenticated backend users to execute arbitrary SQL via the DataObject grid id column filter. The filter value is concatenated directly into the SQL WHERE clause without parameterization. An attacker with backend access can exfiltrate or modify all database contents.	2026-08-11	8.8	CVE-2026-72562
Pinry--Pinry	A server-side request forgery vulnerability in Pinry through 2.1.13 allows unauthenticated remote attackers to make the server issue HTTP requests to arbitrary internal or external hosts via the pin-from-URL feature. The feature passes the user-supplied URL directly to requests.get() without host or IP validation, and ALLOW_NEW_REGISTRATIONS defaults to true enabling anonymous triggering. An attacker can reach internal services or cloud metadata endpoints from the server.	2026-08-11	7.5	CVE-2026-72606

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PluginOps--MailChimp Subscribe Forms	Unauthenticated Cross Site Scripting (XSS) in MailChimp Subscribe Forms <= 4.3.3 versions.	2026-08-13	7.1	CVE-2026-27536
Portainer--Portainer CE	An authentication bypass vulnerability in Portainer CE through 2.44.0 allows authenticated low-privileged users to bypass Docker proxy authorization checks via non-canonical URL normalization, defeating all authorization middleware. The proxy endpoint fails to normalize request paths before applying access controls, allowing crafted requests to be interpreted differently by the proxy and the authorization layer. Successful exploitation grants the attacker root-level access to the underlying Docker host.	2026-08-11	8.8	CVE-2026-72533
PostGIS--address_standardizer	The address_standardizer extension for PostGIS through 3.7.0, fixed in commit 423570b, contains an out-of-bounds write vulnerability that allows a database user with the ability to supply caller-controlled relation names to standardize_address() to trigger memory corruption by providing a rules table with a classification Type value exceeding the fixed class range. Attackers can craft a malicious rules table entry with an oversized rule type value that is used without bounds checking as an index into an internal output-link table, resulting in an out-of-bounds write.	2026-08-13	8.8	CVE-2026-73514
PostGIS--PostGIS	PostGIS before 3.7.0beta2 contains an out-of-bounds read vulnerability that allows attackers to cause memory disclosure or a server crash by supplying a malformed FlatGeobuf buffer. The FlatGeobuf property metadata decoder verifies that a string length field is present but fails to verify that the subsequent string body is contained within the supplied buffer before materializing it into a SQL-visible value, enabling memory disclosure or denial of service.	2026-08-13	8.1	CVE-2026-73515
PostgreSQL--PostgreSQL	Integer wraparound in PostgreSQL tsvector and tsquery data type functions allows an unprivileged database user to cause the server to undersize an allocation and write out-of-bounds, via crafted large inputs. This may execute arbitrary code as the operating system user running the database. These types are typically sourced from application logic, not taken from the application's user. Hence, application users attacking the database, through the application as a conduit, are unlikely. CVE-2026-6473 had fixed similar problems. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-14662
PostgreSQL--PostgreSQL	Heap buffer overflow in PostgreSQL regexp allows the query author to execute arbitrary code as the operating system user running the database, via text that would not pass encoding validation. This shares heritage with CVE-2026-2006, but this case involved unanticipated data growth when round-tripped through pg_wchar. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-14664
PostgreSQL--PostgreSQL	Type confusion regarding input of PostgreSQL ctid data type selectivity estimator allows an object creator to view a calculation derived from the value of an arbitrary 4-byte span of memory, via a chosen non-ctid input. While the calculation loses precision, substantial memory value recovery appears possible. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.1	CVE-2026-14668
PostgreSQL--PostgreSQL	Heap buffer overflow in PostgreSQL to_char(timestampz) allows the party choosing the timezone to execute arbitrary code as the operating system user running the database, via a long POSIX timezone abbreviation. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-14669
PostgreSQL--PostgreSQL	Heap buffer overflow in PostgreSQL plperl return of a tied hash allows the function owner to execute arbitrary code as the operating system user running the database, via a crafted function body. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-14670
PostgreSQL--PostgreSQL	Type confusion in PostgreSQL module "refint" allows an object creator to execute arbitrary code as the operating system user running the database. The fix for this emerged as a non-security bug report, and the fix appear in the git repository with subject "refint: Remove plan cache.", without a CVE number. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-14671
PostgreSQL--PostgreSQL	Heap buffer overflow in PostgreSQL pg_stat_statements allows the query author to execute arbitrary code as the operating system user running the database, via crafted queries containing array constants. Within major version 18, minor versions before PostgreSQL 18.5 are affected. Versions before PostgreSQL 18 are unaffected.	2026-08-13	8.8	CVE-2026-14676
PostgreSQL--PostgreSQL	Integer wraparound in PostgreSQL 32-bit builds of plperl and plperl allows an object creator to cause the server to undersize an allocation and write out-of-bounds via crafted function bodies. This may execute arbitrary code as the operating system	2026-08-13	8.8	CVE-2026-14677

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user running the database. CVE-2026-6473 had fixed similar problems. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.			
PostgreSQL--PostgreSQL	Stack buffer overflow in PostgreSQL argument name matching allows an object creator to achieve unknown impacts via OUT parameter count. The attack can write only 0x0 and 0x1 bytes. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.2	CVE-2026-14679
PostgreSQL--PostgreSQL	Type confusion with PostgreSQL "internal" data type arguments allows any user to execute arbitrary code as the operating system user running the database, via calls to functions with that argument type. Type "internal" represents a class of mutually-incompatible data structures not intended for access from SQL. The system intended to prevent such function calls, but this prevention had gaps. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-14680
PostgreSQL--PostgreSQL	SQL injection in PostgreSQL EXTRACT() deparse allows an object owner to execute arbitrary SQL as a superuser via a hostile object definition. Attacks affect expression deparse consumers broadly, including pg_dump, psql commands like \sf, and any similar usage in non-core tools. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-15741
PostgreSQL--PostgreSQL	Integer wraparound in PostgreSQL fuzzystrmatch allows a user to direct writes to a huge range of addresses, executing arbitrary code as the operating system user running the database, via extreme inputs to SQL function levenshtein() or levenshtein_less_equal(). Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-15742
PostgreSQL--PostgreSQL	Type confusion in PostgreSQL pg_restore_attribute_stats() allows an object creator to execute arbitrary code as the operating system user running the database, via conflation of range and multirange values. Within major version 18, minor versions before PostgreSQL 18.5 are affected. Versions before PostgreSQL 18 are unaffected.	2026-08-13	8.8	CVE-2026-16238
PostgreSQL--PostgreSQL	Type confusion in PostgreSQL "portal"/cursor lifecycle allows a user to execute arbitrary code as the operating system user running the database, via re-creation of a cursor or other portal with different types. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-16239
PostgreSQL--PostgreSQL	Untrusted data inclusion in pg_dump in PostgreSQL allows a malicious superuser of the origin server to inject arbitrary code for restore-time execution as the client operating system account running psql to restore the dump, via psql \restrict meta-command input expansion. The fix for CVE-2025-8714 introduced \restrict and \unrestrict to block this attack, but \unrestrict itself was sufficient for an attack. pg_dumpall is also affected. pg_restore is affected when used to generate a plain-format dump. Non-core use of \restrict would be affected, but we've not identified non-core use. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-18408
PostgreSQL--PostgreSQL	Heap buffer overflow in PostgreSQL pg_dump of long function transform lists allows an object creator to execute arbitrary code as the operating system user running pg_dump, via a crafted transform list. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.8	CVE-2026-19385
PostgreSQL--PostgreSQL	Untrusted data inclusion in PostgreSQL psql COPY may allow a server administrator to elicit execution of data lines as psql commands, via error injection. If the "COPY FROM STDIN" or "\copy FROM STDIN" command fails before the server indicates that it awaits input rows, psql processes the in-line data rows as psql commands. "COPY FROM" with a filename is unaffected. The server administrator has no inherent control over the data rows, so a complete attack requires the attacker to separately acquire control of both the server and the data rows. Alternatively, an attacker controlling data rows alone might complete an attack through a coincidental error that they don't control. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	8.1	CVE-2026-6464
PostgreSQL--PostgreSQL	Missing authorization in PostgreSQL logical decoding allows a non-superuser holding REPLICATION privilege to dlopen any file visible to the operating system account running the server, via the choice of logical decoding plugin. This in turn runs arbitrary code as that account. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	7.2	CVE-2026-6471
powerfulwp--Local Delivery Drivers for WooCommerce	Unauthenticated Cross Site Scripting (XSS) in Local Delivery Drivers for WooCommerce <= 3.0.0 versions.	2026-08-13	7.1	CVE-2026-66468
PrefectHQ--Prefect	An argument injection vulnerability in PrefectHQ Prefect through 3.8.2 allows authenticated users to achieve remote code execution via the git_clone pull step	2026-08-11	8.8	CVE-2026-72538

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	branch field. The branch parameter is passed directly to git pull without sanitization, enabling injection of arbitrary git arguments. This represents a distinct code path from the incomplete fix applied for CVE-2026-5366 and allows command execution on the Prefect server.			
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions)	CWE-287: Improper Authentication	2026-08-13	10	CVE-2026-59500
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions)	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-359: Exposure of Private Personal Information to an Unauthorized Actor	2026-08-13	9.1	CVE-2026-59503
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions)	CWE-602: Client-Side Enforcement of Server-Side Security	2026-08-13	9.1	CVE-2026-59504
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions)	CWE-306: Missing Authentication for Critical Function	2026-08-13	9.3	CVE-2026-59506
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions)	CWE-798: Use of Hard-coded Credentials CWE-200: Exposure of Sensitive Information to an Unauthorized Actor CWE-284: Improper Access Control	2026-08-13	9.3	CVE-2026-59507
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions)	CWE-284: Improper Access Control	2026-08-13	8.2	CVE-2026-59501
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions)	CWE-284: Improper Access Control	2026-08-13	8.6	CVE-2026-59505
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions).	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	2026-08-13	8.6	CVE-2026-59499
Progress Software Corporation--WhatsApp Gold	In WhatsApp Gold versions released before 2026.0.2, an authenticated attacker can bypass frontend controls and inject persistent script content.	2026-08-12	8	CVE-2026-65937
Progress Software Corporation--WhatsApp Gold	In WhatsApp Gold versions released before 2026.0.2, an unauthenticated remote attacker with network access to the affected service can execute arbitrary code in the context of the IIS application service account.	2026-08-12	8.8	CVE-2026-65941
prosolution--ProSolution WP Client	The ProSolution WP Client plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the proSol_fileDeleteProcess function in all versions up to, and including, 2.0.8. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). An attacker must first call the proSol_fileUploadModalProcess handler to poison their own session with a path-traversal key, then call proSol_fileDeleteProcess with that key as the filename parameter; both steps require only the publicly exposed frontend nonce.	2026-08-16	9.1	CVE-2026-14524
prosolution--ProSolution WP Client	The ProSolution WP Client plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 2.0.10 via the proSol_handleFileUpload function. This is due to missing validation of the attacker-controlled Content-Disposition header filename, which overrides the allow-listed multipart filename before the file is saved, and a post-save extension check that fails to delete the	2026-08-16	9.8	CVE-2026-16098

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	already-written file. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible. The nonce required to reach the upload handler is publicly exposed via wp_localize_script on any front-end page rendering the job portal shortcode, allowing unauthenticated visitors to obtain a valid nonce and bypass that gating check entirely.			
prowler-cloud--prowler	Prowler is a cloud security platform. Prior to 5.36.0, the Kubernetes provider connection test accepted kubeconfig_content containing a legacy gcp auth-provider with config.cmd-path and config.cmd-args because kubeconfig_contains_exec_auth in api/src/backend/api/v1/serializers.py checked only exec blocks, and POST /api/v1/providers/{id}/connection loaded it through config.load_kube_config_from_dict in prowler/providers/kubernetes/kubernetes_provider.py, causing kubernetes-python CommandTokenSource.token to run the attacker-supplied command through subprocess.Popen on the shared worker. This issue is fixed in version 5.36.0.	2026-08-12	9.9	CVE-2026-73263
prowler-cloud--prowler	Prowler is a cloud security platform. Prior to 5.33.1, an authenticated user with Lighthouse provider configuration access could supply an unvalidated base_url for the openai_compatible provider through POST /api/v1/lighthouse/providers and POST /api/v1/lighthouse/providers/{id}/connection, causing api/src/backend/tasks/jobs/lighthouse_providers.py to send outbound requests, including the API key in the Authorization header, to attacker-controlled or internal endpoints when client.models.list was called. This issue is fixed in version 5.33.1.	2026-08-12	7.6	CVE-2026-73264
Pulsetto--Vagus Nerve Stimulator	The firmware of the Pulsetto Vagus Nerve Stimulator accepts several undisclosed commands over its Bluetooth Low Energy (BLE) interface. These commands are sent without authentication or encryption, and are never issued by the companion mobile application, yet are fully processed by the device when it is powered on.	2026-08-11	8.1	CVE-2026-18844
Quanovate Tech Inc. (operating as Mira / Mira Care)--Mira Firmware	The distributed Mira Android APK v4.5.15.4 allows an attacker read/write access to reproductive health profiles from internet connected hosts, which could result in forgery, deletion, or destruction of health information.	2026-08-11	9.1	CVE-2026-67568
Quanovate Tech Inc. (operating as Mira / Mira Care)--Mira Firmware	The login endpoint on the Mira cloud API accepts any format-valid string in the password field and returns a live active session token for the account matching the supplied email address. An attacker could use an email address to control cloud accounts and access hormone record information and account settings.	2026-08-11	9.8	CVE-2026-68067
Quanovate Tech Inc. (operating as Mira / Mira Care)--Mira Firmware	In the Mira hormone monitor device firmware v1.7.1.47 build 01070147, a remote unauthenticated attacker within BLE range (approximately 10-30 meters) can silently rebind the device to an attacker-controlled account, extract stored hormone measurements in plaintext, cause a denial-of-service via malformed or undocumented command opcodes, and passively track the user via a static random BLE address that never rotates.	2026-08-11	8.8	CVE-2026-66875
Quanovate Tech Inc. (operating as Mira / Mira Care)--Mira Firmware	The Mira Android companion app v4.5.15.4 identifies the paired Mira hormone analyzer by performing a substring match against the BLE advertisement name only, with no cryptographic peripheral authentication, MAC allowlist, or bonded-identity check. An attacker could capture live session token information and inject forged hormone measurements into the victim's cloud record and clinical trend view.	2026-08-11	7.4	CVE-2026-67558
QuarkA--QA Analytics	Unauthenticated Remote Code Execution (RCE) in QA Analytics <= 5.2.0.0 versions.	2026-08-13	10	CVE-2026-27544
rafasashi--User Session Synchronizer	The User Session Synchronizer plugin for WordPress is vulnerable to Authentication Bypass leading to Account Takeover in all versions up to, and including, 1.4.0. The `synchronize_session()` function, hooked on `init` and therefore executed on every request, performs no nonce, capability, or shared-secret validation against the attacker-supplied `ussync-key`, `ussync-token`, and `ussync-ref` parameters; when `ussync-key` references an unregistered slot, `get_option()` returns `false` for both the secret key and the domain list, causing the AES-256-CBC encryption key to degrade to the fully predictable `md5("")` and the referer allowlist to collapse to an empty-string match, while the AES IV is unconditionally hard-coded as `md5('another-secret')`. This makes it possible for unauthenticated attackers to supply a crafted request encrypting any known or guessable user email address in the `ussync-ref` parameter, causing the handler to call `wp_set_auth_cookie()` for the matched user and granting full authentication as that user - including administrators - with no prior knowledge of site secrets.	2026-08-15	9.8	CVE-2026-15341

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Raisecom--Communication Command and Dispatch Management Platform	A vulnerability was identified in Raisecom Communication Command and Dispatch Management Platform up to 7.6.5. This affects an unknown part of the file /app/users/getpwd.php. Such manipulation of the argument sip leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-14	7.3	CVE-2026-19764
Rapid7--Velociraptor	An authenticated attacker can spoof another GUI user's identity by sending their request with the custom header \"Grpc-Metadata-USER\". This can lead to an account takeover attack from a user with low privileges to administrator.	2026-08-11	9.6	CVE-2026-18972
Rapid7--Velociraptor	Velociraptor allows multi-tenant deployments named \"Orgs\". By default Velociraptor, uses the ROOT org, but users can create child orgs for other tenants within the same deployment. Users can have different permissions in each org. To manage Orgs, Velociraptor usually examines the ORG_ADMIN permission on the ROOT org. This issue results from the Velociraptor server allowing for the deletion of Orgs by incorrectly checking the ORG_ADMIN permission of callers within the calling ORG instead of the ROOT org. However, Org admins of child orgs were able to add this permission to their ACL token within their own org. This allows an administrator in a child org, which is not also an administrator in the ROOT org, to delete other orgs.	2026-08-11	8.7	CVE-2026-18860
Rapid7--Velociraptor	Velociraptor allows scheduling new collections via VQL queries in notebooks. For a user to schedule a new collection, they require the COLLECT_CLIENT permission. However, this is not enforced when the user can run a VQL query which resets the authorization provider. This allows a user who can run arbitrary VQL (usually with the \"analyst\" role) to launch new collections (usually requires the \"investigator\" role). This vulnerability is an escalation from an analyst to investigator role.	2026-08-12	8.2	CVE-2026-64954
Rapid7--Velociraptor	Velociraptor's VQL has a query() plugin which allows running a VQL query in a different org or user context. To be able to run as a different user, the calling user needs to have the IMPERSONATE permission (usually only given to administrators). Velociraptor versions prior to 0.77.2 evaluate this permission against the caller's org instead of against the target org. This allows an administrator in one org to impersonate another user in another org, in which they may not have the IMPERSONATE permission.	2026-08-11	7.2	CVE-2026-18635
Rapid7--Velociraptor	When Velociraptor is configured to use an OIDC IdP for authentication, it uses the email claim as a username. However, some IdP allow users to change the email claim without verification. Some IdPs do not set the \"email_verified\" claim and do not actually verify the email. This allows a user to impersonate another user by setting their email address within the IdP, allowing account takeover.	2026-08-11	7.3	CVE-2026-18639
Rapid7--Velociraptor	The NewNotebook API does not sufficiently sanitize its parameters allowing an authenticated user with NOTEBOOK_EDIT permission to write the notebook record outside the org's data store directory. The file written must have an extension of \".json.db\" but can otherwise overwrite other metadata files (such as ACL records, hunts etc). This can corrupt these files and cause data corruption.	2026-08-11	7.1	CVE-2026-18640
Razinsoft--Ready eCommerce	ReadyCommerce before 4.5.2 contains an unauthenticated SQL injection vulnerability in the product listing API where the rating parameter from the products endpoint is concatenated directly into a MySQL HAVING clause without parameterization in ProductController.php. Attackers can perform time-based blind SQL injection through the unsanitized rating parameter to extract the full database contents, including user credentials and administrator password hashes, with potential additional file system access due to the database connection running as root.	2026-08-10	9.8	CVE-2026-63106
RealMag777--Active Products Tables for WooCommerce	Unauthenticated SQL Injection in Active Products Tables for WooCommerce <= 1.1.1 versions.	2026-08-13	9.3	CVE-2026-66436
Red Hat--Multicluster Engine for Kubernetes	A flaw was found in the cluster-curator-controller component of multicluster engine (MCE). A tenant with create or update permissions on ClusterCurator resources can inject an arbitrary Job specification. This is possible because the CreateJob() function does not validate user-controlled input when unmarshaling the spec.install.overrideJob raw extension. Successful exploitation allows the injected Job to run with the controller's elevated privileges, leading to arbitrary code execution and privilege escalation, potentially accessing cluster-wide secrets.	2026-08-12	9.9	CVE-2026-73268
Red Hat--Multicluster	A flaw was found in the cluster-curator-controller component. A local user, by creating a ClusterCurator resource with a specific naming convention, can trigger the creation of a cluster-scoped ClusterRoleBinding. This allows the user to	2026-08-12	9.9	CVE-2026-73269

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Engine for Kubernetes	escalate their privileges from namespace-local access to cluster-wide control. This privilege escalation grants broad permissions, including the ability to access and manipulate secrets, manage cluster actions, and delete hosted clusters or node pools.			
Red Hat--Multicloud Engine for Kubernetes	A flaw was found in the clusterclaims-controller component of Multicloud Engine (MCE). An authenticated tenant can exploit this vulnerability by manipulating ClusterClaim labels. This allows the tenant to force a cluster to join a ManagedClusterSet belonging to another tenant. Such unauthorized access could enable the injection of policies and workloads into other tenants' clusters.	2026-08-13	7.1	CVE-2026-73266
Red Hat--Multicloud Global Hub	A flaw was found in multicloud-global-hub. The manager component improperly validates the source identity of incoming CloudEvents on Kafka status topics. A remote attacker, after compromising a managed hub and obtaining its Kafka client certificate, can manipulate the self-asserted source identity. This allows the attacker to falsify or delete critical data, such as compliance, inventory, and cluster health information, belonging to other hubs in the database.	2026-08-10	8.5	CVE-2026-71576
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in multicloud-integrations, a component of Red Hat Advanced Cluster Management (RHACM). This vulnerability allows an authenticated user, referred to as a tenant, to manipulate the GitOpsCluster controller. By exploiting this, a tenant can redirect sensitive spoke cluster bearer tokens from secure locations to a namespace they control. This unauthorized access to tokens can lead to the disclosure of critical information and bypass security policies within ArgoCD AppProjects.	2026-08-12	9.6	CVE-2026-70398
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in acm-search-v2-rhel9. An attacker with administrative privileges on the hub cluster, specifically with patch access to the Search Custom Resource (CR), could exploit a vulnerability in the `Collector.ImageOverride` field. This allows the attacker to deploy an arbitrary container image across all managed clusters. The consequence is remote code execution (RCE), enabling the attacker to execute commands and potentially access sensitive information across the entire fleet of managed clusters.	2026-08-12	9	CVE-2026-71471
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the multicloud-operators-subscription component of Red Hat Advanced Cluster Management (RHACM). This vulnerability allows a namespace-admin tenant to perform a confused-deputy attack by creating Subscription Custom Resources (CRs) that leverage a highly privileged ServiceAccount (SA). This enables the tenant to deploy arbitrary cluster-scoped resources, leading to privilege escalation and potential arbitrary code execution across the cluster.	2026-08-12	9.9	CVE-2026-72508
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the multicloud-integrations component. The Application propagation controller processes the `ocm-managed-cluster` annotation from an Application Custom Resource (CR) without proper validation. A tenant with permissions to create Applications on the hub cluster can exploit this to target arbitrary managed clusters. This can force ArgoCD on the spoke clusters to synchronize attacker-controlled manifests, leading to arbitrary code execution or privilege escalation on those clusters.	2026-08-12	9.9	CVE-2026-72526
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the `search-v2-operator` component. A user with specific administrative permissions on a managed cluster can exploit a vulnerability that allows them to inject arbitrary configuration data. This manipulation can override critical settings, leading to the replacement of container images. This ultimately results in container image injection on the managed cluster, potentially compromising its integrity.	2026-08-12	8.5	CVE-2026-71473
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in multicloud-operators-subscription. A privileged user, specifically a namespace administrator capable of creating Channel and Subscription resources, can exploit this vulnerability. By manipulating the Channel.Spec.SecretRef.Namespace field, the user can cause the system to copy sensitive Secret contents from other namespaces into their own, leading to information disclosure.	2026-08-12	7.7	CVE-2026-66878
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in search-v2-api. The authentication middleware in the affected component unconditionally skips authentication when a request includes an `Upgrade: websocket` header. An unauthenticated attacker can exploit this by sending a specially crafted HTTP POST request to the `/federated` endpoint with the `Upgrade: websocket` header. This allows the attacker to bypass authentication and access federated search results across all configured remote managed hubs, leading to information disclosure.	2026-08-11	7.5	CVE-2026-71467
Red Hat--Red Hat Advanced Cluster	A flaw was found in search-v2-api. An unauthenticated attacker can exploit this by sending requests with unique random bearer tokens. Each unique token creates a permanent entry in the unbounded tokenReviews cache, which is not properly	2026-08-12	7.5	CVE-2026-71469

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management for Kubernetes 2	cleared. This can lead to memory exhaustion of the search-api pod, resulting in a Denial of Service (DoS).			
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the multicloud-operators-channel component of Red Hat Advanced Cluster Management (RHACM). This vulnerability allows a compromised agent from a managed cluster to gain unauthorized access to sensitive information. Specifically, the agent can read all Secrets and ConfigMaps within any Channel namespace on the hub, potentially exposing credentials for other tenants' Git and Helm repositories. This could lead to significant information disclosure.	2026-08-12	7.7	CVE-2026-73122
Red Hat--Red Hat Container Native Virtualization 4.12	A symlink following vulnerability was found in KubeVirt's virt-handler migration proxy. During live migration, virt-handler dials Unix sockets inside the target virt-launcher pod via /proc/<pid>/root/ paths using net.Dial() without symlink protection. These socket paths reside in qemu-owned directories writable by the virt-launcher user. An attacker with namespace edit and pods/exec permissions can replace a migration proxy socket with a symlink to the host CRI-O socket. Because virt-handler runs as root in the host mount namespace, absolute symlink targets resolve against the host filesystem, and the bidirectional io.Copy proxy relays attacker-controlled bytes to the container runtime, enabling full node compromise.	2026-08-12	8.8	CVE-2026-13622
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in DBI. This is a fix for a partial fix for CVE-2026-14380 for RHEL 9.8.z and 10.2.z. For a detailed Statement, Description and Mitigation please refer to the original https://access.redhat.com/security/cve/cve-2026-19546 .	2026-08-11	8.8	CVE-2026-19546
Red Hat--Red Hat Enterprise Linux 10	A heap out-of-bounds write vulnerability was found in the GStreamer gst-plugins-bad adpcmdec element when decoding IMA/DVI ADPCM audio. Insufficient validation of the per-block sample count for multi-channel streams allows a crafted WAV file to cause writes beyond the allocated output buffer. This can lead to application crash, denial of service, memory corruption, or potentially arbitrary code execution when untrusted media is processed.	2026-08-10	7.6	CVE-2026-19387
Red Hat--Red Hat Enterprise Linux 10	Multiple integer overflow and underflow vulnerabilities were found in the GStreamer gst-plugins-ugly ASF demuxer (asfdemux) when parsing header objects from crafted ASF, WMV, or WMA files. Insufficient validation of attacker-controlled length and size values can bypass bounds checks and cause out-of-bounds heap reads. This can result in application crash, denial of service, or limited information disclosure when untrusted media is processed.	2026-08-10	7.1	CVE-2026-19389
Red Hat--Red Hat Enterprise Linux 10	A unauthenticated remote peer may lead rsyslogd to crash due to a flaw in the optional imtcp module. A crafted input sequence during oversize-frame recovery can cause an invalid internal message length and terminate rsyslogd. No confidentiality or integrity impact, privilege escalation, or code execution has been identified. imtcp and the default imtcp framing modes are not affected.	2026-08-12	7.5	CVE-2026-19654
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in libvirt. A local attacker, specifically a process running as the confined `swtpm` user, could exploit a symlink-following vulnerability in the `virFileChownFiles()` function. By planting a symbolic link within the `swtpm` state directory, the attacker could trick the root-level libvirt daemon into changing the ownership of an arbitrary file to the `swtpm` user. This allows for privilege escalation from the `swtpm` sandbox to root-level file ownership control.	2026-08-10	7.8	CVE-2026-63622
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in iperf3. A remote attacker can exploit this vulnerability by sending crafted control-channel JSON with oversized numeric parameters, such as `parallel` and `len`, which are not properly validated by the server. This improper input validation can lead to excessive stream and thread creation, as well as large buffer allocations, causing resource exhaustion. Consequently, this can result in a Denial of Service (DoS) on the affected iperf3 server.	2026-08-11	7.5	CVE-2026-71217
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in MRTG. When the MRTG daemon is started as a root user and subsequently drops privileges, a local, low-privileged attacker can exploit a symbolic link (symlink) following vulnerability. By influencing or pre-placing a symlink in the process ID (PID) file path, the attacker can trick the root process into changing the ownership of an arbitrary existing file to the daemon user. This can lead to local privilege escalation, allowing unauthorized access to or modification of sensitive files.	2026-08-11	7.1	CVE-2026-72694
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in GIMP's PSD file format plugin. This vulnerability, an unsigned integer underflow in the `block_rem` variable, occurs when a user opens a specially crafted `.psd` image file. The underflow leads to parser confusion, enabling an attacker to inject arbitrary data as layer resource blocks. This can ultimately result in arbitrary code execution, allowing the attacker to run malicious code on the victim's system.	2026-08-10	8.4	CVE-2026-59090

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in the GIMP image manipulation program, specifically within its Seattle Filmworks file loader. A remote attacker could exploit this vulnerability by tricking a user into opening a specially crafted Seattle Filmworks file. This could lead to a heap overflow, allowing the attacker to write several kilobytes of controlled data beyond the intended memory buffer. Such an overflow can result in memory corruption, potentially leading to arbitrary code execution or a denial of service.	2026-08-10	7.8	CVE-2026-59087
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in GIMP's file format plugins, including those for PSD and PAA files. A remote attacker could exploit these vulnerabilities by tricking a user into opening a specially crafted image file. This could lead to unexpected application behavior or other potential security impacts without requiring further user interaction.	2026-08-10	7.3	CVE-2026-59091
Red Hat--Red Hat Hardened Images	'openvt -u' is intended to identify the owner of the current VT and then execute 'login' as that user from a privileged context. In the documented 'kbrequest'/init usage, the ownership test in 'authenticate_user()' relies on 'stat("/proc/<pid>/fd/0")'. 'stat()' on '/proc/<pid>/fd/0' follows the symlink to the underlying TTY device node. As a result, 'buf.st_uid' reflects the owner of the TTY node rather than the owner of the process holding the file descriptor. If the TTY owner returns to 'root' or the getty owner after logout while an unprivileged process still has 'fd 0' attached to that TTY, the check can incorrectly treat that process as belonging to the privileged console owner. Once that check succeeds, the '-u' path executes a passwordless login as the selected user. In the documented 'kbrequest'/init deployment using 'openvt -us', this can result in passwordless 'login -f root' on the spawned VT. This report establishes that privilege escalation path for that documented deployment; it does not claim equivalent reachability for deployments that do not use 'openvt -u' from a privileged 'kbrequest'/init path.	2026-08-11	7.8	CVE-2026-72693
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	A flaw was found in Picketlink Federation SAML; the unsolicited response handler would accept forged assertions with no verification or validation, permitting an unauthed attacker to authenticate as any principal in any role. This could lead to information disclosure, access to restricted operations, or other flaws.	2026-08-11	9.8	CVE-2026-10579
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	A flaw was found in JBoss marshalling. The Infinispan session replication path deserializes replicated session data via the JBoss Marshalling River unmarshaller with no class filtering - enabling RCE via deserialization gadget chains on every cluster node.	2026-08-11	8.8	CVE-2026-15555
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	A flaw was found in Picketlink's SP signature validation; a SAML response containing zero assertion elements matching the signature check can allow an attacker to forge a SAML response and auth as any principal with any roles on the protected application.	2026-08-11	8.1	CVE-2026-15556
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	when EAP runs with -secmgr, the openjdk-orb's JDKBridge honours attacker-supplied CDR codebase URLs during object unmarshalling on :3528, allowing an unauthenticated attacker to load and instantiate arbitrary classes from a remote URL in the server JVM before EJB security interceptors run.	2026-08-11	8.1	CVE-2026-15560
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	the Undertow AJP listener honours forged ssl_cert and is_ssl AJP attributes without requiring any shared-secret authentication. This enables an unauthenticated attacker with direct TCP access to port 8009 to bypass CLIENT-CERT authentication by injecting a forged X.509 certificate via the AJP protocol.	2026-08-11	7.4	CVE-2026-15554
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	A flaw was found in EAP's undertow http/1.1 chunked-transfer decoder. missing limits on size and count would allow an attacker to use an unauthenticated connection to drive the JVM to an OutOfMemory error, stopping all deployments on the listener, and achieving Denial of Service.	2026-08-11	7.5	CVE-2026-15561
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	A flaw was found in EAP's jboss-remoting. A remote unauthenticated attacker who can reach :8080 (or :9990, or :4447) and complete an Upgrade: jboss-remoting handshake can cause OOM errors that degrade requests server-wide, leading to denial of service.	2026-08-11	7.5	CVE-2026-15562
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	A flaw was found in EAP's IIOP. The listener's NameService would accept bind operations without authentication, allowing an attacker to hijack JNDI lookups and binding them to a malicious ORB, achieving MITM or DoS on further invocations.	2026-08-11	7.4	CVE-2026-15563
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	A flaw was found in Undertow. A remote attacker can cause Out of Memory on websockets endpoint without authentication on any @ServerEndpoint class that has any @OnMessage method. This allows an attacker to cause Denial of Service attack without authentication and using only a standard WebSocket handshake.	2026-08-11	7.5	CVE-2026-15565

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat JBoss Enterprise Application Platform 7.4.25	A flaw was found in Wildfly. A remote unauthenticated attacker can trigger OutOfMemoryError as CSlv2Util's GSS token decoder reads an attacker-controlled length field without bounds checking and attempts to allocate a byte array of that size.	2026-08-11	7.5	CVE-2026-15567
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in Feast. The system improperly deserializes user-defined functions (UDFs) stored in its registry, which are serialized using the 'dill' library. This allows a remote attacker to store a malicious UDF, leading to unauthenticated arbitrary code execution on the feature server in default configurations. An authenticated attacker can also achieve arbitrary code execution on the registry server by bypassing authorization checks during deserialization. This vulnerability can result in cross-tenant data access and lateral movement within the system.	2026-08-10	9.9	CVE-2026-18948
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in the trustyai-service-operator's LMEvalJob controller. An authenticated user within the cluster can exploit this vulnerability by configuring a sidecar container to bypass existing security policies. This allows the user to enable and execute untrusted remote code, leading to arbitrary code execution within the cluster.	2026-08-10	8.1	CVE-2026-15467
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in the TrustyAI Service (TAS) deployment. This vulnerability allows any pod on the cluster network to bypass authentication and directly access the TAS backend API. An attacker can exploit this to read, tamper with, or delete monitoring data and configurations, and inject arbitrary data into the service, potentially disrupting tenant operations.	2026-08-10	8	CVE-2026-15581
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in the Data Science Pipelines Operator (DSPO). The operator's ClusterRole, which defines its permissions, includes extensive privileges beyond what is necessary for its operation. These excessive permissions, such as the ability to execute commands within pods and manage cluster-wide roles, could be exploited. If the DSPO pod were compromised, an attacker could leverage these privileges to gain full administrative control over the entire Kubernetes cluster.	2026-08-10	8.7	CVE-2026-18608
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in the Data Science Pipelines Operator (DSPO). A namespace editor can exploit a vulnerability in the spec.database.customExtraParams field, which allows for the injection of dangerous parameters into the MySQL Data Source Name (DSN) string. By manipulating these parameters, an attacker can enable LOCAL INFILE functionality and exfiltrate sensitive files, such as the service account token, from the operator pod. This can lead to privilege escalation, allowing a namespace editor to gain cluster-admin privileges.	2026-08-10	8.8	CVE-2026-18617
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in Feast. An authorization bypass vulnerability exists in the /materialize and /materialize-incremental endpoints. By sending a specially crafted request that omits the feature_views field, an attacker can bypass intended permission checks. This allows an unauthenticated remote attacker, or any authenticated user, to trigger a full re-materialization of all feature views. The consequence is a Denial of Service (DoS) due to data corruption and significant resource consumption across all tenants.	2026-08-10	8.5	CVE-2026-18947
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in odh-dashboard. This vulnerability allows an attacker, who has compromised the dashboard's Service Account (SA) token, to exploit overly broad permissions granted to the SA. This enables the attacker to escalate their privileges to cluster-administrator level, gain access to sensitive data like credentials and keys across the entire cluster, and disrupt multi-tenant isolation.	2026-08-10	8.8	CVE-2026-18949
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in odh-dashboard. An authenticated user of the dashboard can exploit a vulnerability related to how RoleBindings are created. The system does not properly validate the `roleRef` field, allowing a user to specify an arbitrary role, including highly privileged ones like `cluster-admin`. This can lead to privilege escalation, where an attacker gains unauthorized elevated access within their namespace and potentially persistent control over the system.	2026-08-10	8.8	CVE-2026-18950
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in the RHOAI training-operator. This vulnerability allows a user with standard edit or admin roles in any Kubernetes namespace to escalate their privileges. Through the creation of training jobs, an attacker can impersonate service accounts, access the host filesystem, and potentially execute arbitrary code remotely. This issue arises from the aggregation of training job permissions onto native Kubernetes edit and admin ClusterRoles, coupled with unrestricted PodTemplateSpec passthrough.	2026-08-10	8.8	CVE-2026-18982
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in the Data Science Pipelines Operator. This vulnerability allows an unauthenticated attacker to derive sensitive credentials, such as MariaDB root/user passwords and MinIO access/secret keys, if they can access the MinIO Route or MariaDB Service. The flaw occurs because the operator uses a cryptographically weak pseudo-random number generator (PRNG) to generate	2026-08-10	7.5	CVE-2026-18611

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	these credentials, making them predictable. Successful exploitation could lead to unauthorized access to all pipeline artifacts and metadata, resulting in significant information disclosure.			
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in ml-metadata. The statically-linked gRPC stack in ml-metadata is outdated, making it vulnerable to known HTTP/2 denial of service (DoS) issues. An in-cluster attacker, with network access to the MLMD pod, could exploit these vulnerabilities by sending specially crafted HTTP/2 requests. This could lead to a denial of service by crashing the MLMD pod, disrupting all pipeline runs in the affected namespace.	2026-08-10	7.5	CVE-2026-18618
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in Data Science Pipelines. A restricted user, or tenant, can exploit an improper authorization vulnerability in the setDefaultServiceAccount function. By specifying a more privileged ServiceAccount (SA) during a CreateRun request, an attacker can bypass authorization checks. This allows the tenant to run their containers with elevated privileges, potentially leading to the disclosure of sensitive information (secrets) and the ability to execute commands within other users' pods.	2026-08-10	7.1	CVE-2026-18620
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in Data Science Pipelines (DSP). An attacker with namespace editor privileges can bypass security hardening by submitting a malicious Argo Workflow through the V1 API path. This allows the API server to create pods with elevated privileges, acting as a 'confused deputy' on behalf of the attacker. Successful exploitation grants the attacker node-root access, enabling arbitrary code execution and full control over the underlying node.	2026-08-10	7.6	CVE-2026-18621
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in Feast and feast-operator. The default configuration for both the Feast SDK and the feast-operator is "no_auth," meaning no security manager is installed. This default allows unauthenticated and unauthorized access to feature-server, registry-server, and offline-server endpoints. A remote attacker, by exploiting this missing authentication, could achieve remote code execution (RCE) by storing a malicious User-Defined Function (UDF) on the feature-server, trigger a denial of service (DoS) by forcing re-materialization of all tenant features, and gain unauthorized access to cross-tenant data.	2026-08-10	7.7	CVE-2026-18941
Red Hat--Red Hat OpenShift AI 3.3	A flaw was found in the Red Hat OpenShift AI (RHOAI) overlay for the training operator. The RHOAI overlay incorrectly aggregates 'trainjobs' management permissions into the native Kubernetes 'edit ClusterRole'. This allows any user with 'edit ClusterRole' permissions in a namespace to create, modify, and delete 'TrainJobs'. When combined with a separate vulnerability (TRN-01) that permits arbitrary pod configurations, a remote attacker with namespace editor privileges could exploit this to escalate privileges, potentially leading to arbitrary code execution.	2026-08-10	8.8	CVE-2026-18951
Red Hat--Red Hat OpenShift AI 3.4	A flaw was found in the MaaS API. This vulnerability allows any pod within the cluster to bypass the Kuadrant AuthPolicy gateway by forging HTTP headers, specifically 'X-MaaS-Username' and 'X-MaaS-Group', which are trusted verbatim. This lack of first-party authentication enables an attacker to gain unauthorized access and escalate privileges. The concrete consequences include the ability to mint Kubernetes ServiceAccount tokens in other tenants' namespaces, revoke API keys, and exfiltrate sensitive model access configuration.	2026-08-10	9.9	CVE-2026-14450
Red Hat--Red Hat OpenShift AI 3.4	A flaw was found in the Red Hat OpenShift AI (RHOAI) MaaS Gateway. Improper configuration of the Gateway in a model-serving context allows a standard user with low privileges to intercept, read, log, and alter all MaaS model traffic. This includes sensitive information such as access keys, input prompts, and outputs, leading to significant information disclosure and data tampering.	2026-08-10	8.8	CVE-2026-13717
Red Hat--Red Hat OpenShift Container Platform 4	An authenticated SSRF flaw was found in the OpenShift Console Dev Console webhook helpers. User-supplied target URLs are fetched server-side without validation, with path neutralization enabling arbitrary endpoint targeting and full response reflection from the console pod's privileged network position.	2026-08-11	7.4	CVE-2026-50236
Red Hat--Red Hat OpenShift Container Platform 4	A Server-Side Request Forgery and supply chain flaw was found in the OpenShift Console Helm catalog proxy. A namespace tenant can plant a ProjectHelmChartRepository with an arbitrary URL that the console pod fetches server-side, bypassing tenant egress restrictions. Combined with catalog metadata poisoning and admin-mediated chart installation, this enables privilege escalation.	2026-08-11	7.4	CVE-2026-50237
Redis--Redis	An out-of-bounds read vulnerability in Redis through 8.8.1 allows an adjacent unauthenticated attacker to cause denial of service or information disclosure by sending a specially crafted PING message to the Redis Cluster Bus port.	2026-08-10	7.1	CVE-2026-72568
reputeinfosystems --Contact Form,	The Contact Form, Survey, Quiz & Popup Form Builder - ARForms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including,	2026-08-16	9.8	CVE-2024-13784

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Survey, Quiz & Popup Form Builder ARForms	1.8.5 via deserialization of untrusted input from form submissions. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.			
Roland Barker--Participants Database	Unauthenticated Arbitrary File Deletion in Participants Database <= 2.7.8.4 versions.	2026-08-13	7.4	CVE-2026-28189
RsyncProject--rsync	rsync daemon before 3.5.0 contains an IP address spoofing vulnerability that allows unauthenticated remote attackers to bypass IP-based access controls by sending a crafted PROXY protocol header with a forged source address. Attackers who can connect directly to the rsync daemon can inject a spoofed source IP in the PROXY protocol header to circumvent hosts allow/deny rules, gaining unauthorized access that would otherwise be blocked based on their real source address.	2026-08-13	9.1	CVE-2026-53791
RsyncProject--rsync	rsync before 3.5.0 contains a time-of-check to time-of-use (TOCTOU) race condition vulnerability in the rrsync restricted shell wrapper that allows authenticated clients to escape enforced directory restrictions by substituting a symlink for a path component after validation but before transfer processing. Attackers can additionally leverage unrestricted flags such as --copy-unsafe-links, -D, and --log-file through rrsync to read or write files outside the permitted directory subtree.	2026-08-13	8.1	CVE-2026-53783
RsyncProject--rsync	rsync before 3.5.0 contains multiple command and argument injection vulnerabilities that allow attackers to execute arbitrary commands by supplying malicious input through several code paths, including the RSYNC_CONNECT_PROG environment variable, daemon hooks, the rsync-ssl wrapper, and remote-shell command newline injection. Attackers can inject shell metacharacters or newline characters into unsanitized user-supplied values such as hostnames and hostsspecs to execute arbitrary commands under the privileges of the rsync process or the invoking user.	2026-08-13	8.1	CVE-2026-53790
RsyncProject--rsync	rsync before 3.5.0 contains an arbitrary file write vulnerability that allows attackers to write files outside the intended destination tree by specifying an absolute path via --temp-dir or --link-dest options. The rename-confinement logic is bypassed when these options resolve to paths outside the destination tree, enabling attacker-controlled values to write files to arbitrary locations accessible to the rsync process.	2026-08-13	8.1	CVE-2026-53795
RsyncProject--rsync	rsync 3.2.0 through 3.2.3 (openssl mode) and rsync-ssl through 3.4.4 (stunnel mode) contain a TLS certificate validation vulnerability that allows on-path attackers to intercept encrypted sessions by presenting self-signed or otherwise invalid certificates. Attackers can exploit the failure to validate server TLS certificates against a trusted CA or verify certificate hostname matching to decrypt or tamper with rsync session content without detection by the client.	2026-08-13	8	CVE-2026-70454
RsyncProject--rsync	rsync 3.0.1 before 3.5.0 contains an out-of-bounds write vulnerability in the read_args() function that allows a malicious sender to corrupt adjacent heap memory by sending a crafted argument list. When the argument count causes the argv allocation to be exactly full, the trailing NULL terminator is written one slot beyond the allocation boundary, corrupting adjacent heap memory.	2026-08-13	8.2	CVE-2026-70456
RsyncProject--rsync	rsync 3.0.0 before 3.5.0 contains an out-of-bounds write vulnerability that allows attackers to corrupt memory by triggering HLINK_BUMP processing on file entries with the FLAG_HLINKED flag set while the hard-link preservation option is inactive. Attackers can exploit the missing F_SUM field in the file_struct layout to access memory past the end of the allocated structure, corrupting adjacent heap or stack data.	2026-08-13	8.2	CVE-2026-70458
RsyncProject--rsync	rsync 2.3.3 before 3.5.0 contains a path traversal vulnerability that allows a malicious sender to escape the module root by exploiting symlinks within the module file tree when using --partial-dir or --backup-dir options. Attackers with write access to place a symlink under the module root, or who can exploit a pre-existing trusted symlink, can direct file writes to locations outside the intended module root, achieving arbitrary file write relative to the module root parent.	2026-08-13	8.1	CVE-2026-70460
RsyncProject--rsync	rsync 3.2.5 before 3.5.0 contains a heap out-of-bounds write vulnerability that allows remote unauthenticated attackers to write one attacker-controlled byte past the end of a heap allocation by supplying a crafted files-from entry. Attackers can trigger the vulnerability against a read-only rsync daemon module by providing	2026-08-13	8.2	CVE-2026-70461

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a files-from entry containing both an interior and trailing backslash, causing the add_implied_include() function to under-count the trailing backslash when sizing the destination buffer.			
RsyncProject--rsync	rsync 3.1.0 before 3.5.0 contains an authorization bypass in auth users directive parsing. The auth users parser uses comma-only tokenization when splitting the user list, which fails to correctly handle entries of the form @Group Name where the group name contains a space. The space within the group name causes the parser to split the entry at the space boundary, discarding the deny rule associated with the group. An authenticated user whose username or group membership would be denied by an @Group Name auth users entry can connect to a restricted module because the deny rule is silently discarded during parsing.	2026-08-13	8.1	CVE-2026-70463
RsyncProject--rsync	rsync before 3.5.0 contains a path traversal vulnerability that allows remote clients to access files outside the intended module root when use chroot is disabled and the module root path or a component of it is a symlink. The daemon calls chdir() to the module root at session initialization without resolving symlinks via realpath() or equivalent, causing subsequent relative-path operations to reference files relative to the symlink target rather than the intended module root, enabling unauthorized file access.	2026-08-13	7.1	CVE-2026-53784
RsyncProject--rsync	rsync before 3.5.0 contains a path traversal vulnerability that allows a malicious sender to write files outside the intended destination directory tree by crafting relative paths with symlink components in --relative mode. The make_path() function follows symlinks pointing outside the destination tree while creating intermediate directories without verifying that created paths remain within the destination boundary, enabling arbitrary file writes on the receiver's filesystem.	2026-08-13	7.1	CVE-2026-53785
RsyncProject--rsync	rsync before 3.5.0 contains a path confinement bypass vulnerability that allows remote clients to escape the intended inner-module root confinement by constructing paths that resolve outside the chroot boundary when the module root contains a ./ boundary marker. Attackers can exploit improper handling of the ./ notation or forge delta-basis transfers referencing xname paths that cross the ./ boundary to gain unauthorized read or write access to files outside the module's subtree.	2026-08-13	7.4	CVE-2026-53793
RsyncProject--rsync	rsync before 3.5.0 contains an arbitrary file read vulnerability that allows attackers to read files accessible to the rsync daemon process by exploiting symlink following in input configuration file handling including --files-from, --password-file, and filter merge files. Attackers can place a symlink at a predictable --files-from or --password-file path, or supply a --files-from path that escapes the daemon module root, to read arbitrary files accessible to the rsync process.	2026-08-13	7.1	CVE-2026-53802
RsyncProject--rsync	rsync before 3.5.0 contains a symlink following vulnerability that allows local attackers to overwrite arbitrary files by placing a symlink at a predictable output path such as --log-file, --write-batch, or daemon-mode log and statistics paths. Attackers can exploit rsync's failure to reject symlinks during ancillary file writes to redirect output to arbitrary filesystem locations, achieving local privilege escalation on installations where rsync runs with elevated privileges such as setuid or privileged daemon configurations.	2026-08-13	7.8	CVE-2026-53803
RsyncProject--rsync	rsync 3.1.0 before 3.5.0 contains an access control bypass vulnerability that allows remote attackers to circumvent hosts deny rules by inducing DNS resolution failures during hostname-based access control evaluation. When a DNS lookup for a hostname-based deny rule fails, the daemon skips the rule rather than defaulting to a deny decision, enabling attackers who can trigger DNS failures to bypass module-level IP access controls and gain unauthorized access to restricted module file trees.	2026-08-13	7.4	CVE-2026-70452
RsyncProject--rsync	rsync before 3.5.0 contains an algorithmic complexity vulnerability in the hash_search() function that allows a remote attacker to cause a denial of service by delivering a carefully constructed file list. A sender can exploit the quadratic-time worst-case behavior in hash lookups to exhaust receiver CPU resources with a modest number of crafted entries, causing a sustained denial of service.	2026-08-13	7.5	CVE-2026-70453
RsyncProject--rsync	rsync 3.4.2 before 3.5.0 contains a denial of service vulnerability that allows a remote sender to exhaust system resources by specifying the --zt short alias for --compress-threads, which bypasses the refuse options directive's string matching on long option names. Attackers can specify --zt=N with a large value to spawn an unbounded number of Zstandard worker threads on the receiver, exhausting available thread and memory resources.	2026-08-13	7.5	CVE-2026-70455
RsyncProject--rsync	rsync daemon 2.0.0 before 3.5.0 contains a denial of service vulnerability that allows unauthenticated remote attackers to exhaust daemon connection slots by	2026-08-13	7.5	CVE-2026-70464

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stalling the handshake process before or after module selection without triggering the I/O timeout. Attackers can open many simultaneous connections and trickle data at the minimum rate to avoid timeout, or stall entirely before module selection where no timeout applies, consuming all available connection slots and denying service to legitimate clients.			
rtCamp--Log in with Google	Unauthenticated Broken Authentication in Log in with Google <= 1.4.2 versions.	2026-08-13	9.8	CVE-2026-28185
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. RustFS AddServiceAccount in rustfs/src/admin/handlers/service_account.rs accepts an attacker-controlled target_user after only checking CreateServiceAccountAdminAction, passes it to new_service_account, and prepare_service_account_auth sets is_owner for the resulting root-parent service account. This issue is fixed in version 1.0.0-beta.11.	2026-08-12	8.8	CVE-2026-73284
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.12, RustFS get_condition_values folds attacker-controlled request headers from HeaderMap into server-derived userid, username, principaltype, groups, versionid, signatureversion, jwt:, and ldap: condition keys, allowing authenticated callers to satisfy identity-based policy conditions. This issue is fixed in version 1.0.0-beta.12.	2026-08-12	8.1	CVE-2026-73286
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.12, RustFS evaluates the ForAllValues: and ForAnyValue: set qualifiers with the negated string operators StringNotEquals, StringNotEqualsIgnoreCase, StringNotLike, ArnNotEquals, and ArnNotLike using each other's semantics because crates/policy/src/policy/function/string.rs negates the aggregate result after eval or eval_like instead of negating each request-value predicate before quantification. Partially overlapping policy and request value sets can therefore make an Allow condition grant access to an excluded principal or make a Deny guardrail fail, including policies based on jwt:groups and jwt:roles; absent keys also receive the opposite ForAllValues: and ForAnyValue: behavior. This issue is fixed in version 1.0.0-beta.12.	2026-08-12	8.1	CVE-2026-73289
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. From 1.0.0-alpha.64 until 1.0.0-rc.1, RustFS external OPA authorization enabled by RUSTFS_POLICY_PLUGIN_URL in crates/iam/src/sys.rs sets PreparedIamAuth.needs_existing_object_tag incorrectly for PreparedIamMode::Opa, causing maybe_merge_object_tag_conditions to omit s3:ExistingObjectTag/* values and allowing authenticated users to bypass tag-based policy restrictions. This issue is fixed in version 1.0.0-rc.1.	2026-08-12	7.5	CVE-2026-73285
s9y--Serendipity	Serendipity before 2.6.0 contains a server-side request forgery vulnerability in the serendipity_url_allowed() filter that fails to block hex-encoded IPv4 addresses, IPv6 literals, and link-local ranges. Authenticated users with adminImagesAdd permission can bypass the filter using alternate address formats to request internal services and retrieve response bodies through the public uploads directory.	2026-08-13	8.5	CVE-2026-73629
sadathimel--MaxUpload Big File Uploads Increase Maximum File Upload Size	The MaxUpload - Big File Uploads - Increase Maximum File Upload Size plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.4.0 via the handle_upload function. This is due to a filename-validation mismatch in the handle_upload function where extension and MIME checks are applied to the uploaded chunk's filename but not to the final assembled filename derived from the resumableFilename parameter. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible.	2026-08-15	8.8	CVE-2026-15965
SAP_SE--SAP ABAP Developer Tools	SAP ABAP Development Tools does not perform necessary authorization checks for certain functionality, allowing an attacker with low privileges to execute unauthorized database operations against SAP NetWeaver AS ABAP. Successful exploitation could allow the attacker to read sensitive data, modify application data, and disrupt access for legitimate users, resulting in high impact on confidentiality, integrity, and availability.	2026-08-11	8.8	CVE-2026-58243
SAP_SE--SAP Business AI Platform (Approuter)	SAP Approuter does not sufficiently validate certain token content under specific configurations. An unauthenticated attacker could send a specially crafted token to cause sensitive credential material to be sent to an attacker-controlled destination. The attack complexity is high due to non-default preconditions required in the target environment. This results in a high impact on confidentiality and a low impact on integrity and availability.	2026-08-11	7	CVE-2026-58230
SAP_SE--SAP BusinessObjects Business	SAP BusinessObjects Business Intelligence Platform stores certain sensitive credentials associated with user objects using a hard-coded cryptographic key. An attacker with high privileges and local access to the server could retrieve these	2026-08-11	7.9	CVE-2026-66763

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Intelligence Platform (Central Management Server)	objects and decrypt the stored credentials. Successful exploitation could allow the attacker to obtain sensitive authentication data and modify protected information, resulting in a high impact on confidentiality and integrity. There is no impact on availability.			
SAP_SE--SAP Commerce Cloud (Data Hub Adapter)	SAP Commerce Cloud allows an unauthenticated attacker to abuse a default authentication client and submit specially crafted input to certain functions lacking sufficient validation. Successful exploitation could enable arbitrary code execution and compromise internal components, resulting in high impact on confidentiality, integrity, and availability of the application.	2026-08-11	10	CVE-2026-58231
SAP_SE--SAP Manufacturing Integration and Intelligence	SAP Manufacturing Integration and Intelligence (MII) allows an attacker with high privileges to submit specially crafted input to certain affected functionality, which is processed without sufficient validation. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system, resulting in high impact on confidentiality, integrity, and availability of the application.	2026-08-11	9.1	CVE-2026-44758
SAP_SE--SAP Manufacturing Integration and Intelligence	SAP Manufacturing Integration and Intelligence allows a privileged attacker to exploit insufficient file path validation in certain functions using specially crafted input. Exploitation also requires a legitimate user to subsequently access the attacker-influenced content and depends on conditions outside the attacker's control. Successful exploitation could allow files to be written outside the intended directory and affect other components, resulting in a high impact on confidentiality, integrity, and availability.	2026-08-11	7.6	CVE-2026-44763
SAP_SE--SAP Manufacturing Integration and Intelligence	Due to a Missing Authorization Check vulnerability in SAP Manufacturing Integration and Intelligence, an unauthenticated attacker could send crafted requests to the Cost Servlet using specific parameter values. If processed by the application, these requests enable access to backend operations. Successful exploitation could allow the attacker to read, create, modify, or delete application-managed business data, resulting in a limited impact on the confidentiality, integrity, and availability of the affected system.	2026-08-11	7.3	CVE-2026-44764
SAP_SE--SAP Manufacturing Integration and Intelligence	Due to a Missing Authorization Check vulnerability in SAP Manufacturing Integration and Intelligence, an unauthenticated remote attacker could access scheduling-related application functions without proper authorization validation. Successful exploitation could allow the attacker to retrieve, create, modify, or delete application-managed scheduling data, causing a low impact on confidentiality, integrity, and availability.	2026-08-11	7.3	CVE-2026-44765
SAP_SE--SAP NetWeaver and ABAP Platform	SAP NetWeaver Application Server ABAP allows an unauthenticated attacker to exploit logical errors in DIAG protocol parsing, resulting in memory corruption. This vulnerability could potentially disclose sensitive system information or crash the system, leading to a high impact on the confidentiality, integrity, and availability of the application.	2026-08-11	9.8	CVE-2026-34265
Saurus--Saurus CMS Community Edition	A CMS contains a SQL injection vulnerability in admin/db_data.php at line 509 that allows authenticated administrators to inject arbitrary SQL into a SHOW COLUMNS FROM statement by supplying unsanitized input through the table_name GET or POST parameter. Attackers can perform table traversal, time-based blind, boolean-based blind, and error-based injection techniques to enumerate full database schema, access system tables such as information_schema, and chain the disclosure with secondary injection points to extract credential data.	2026-08-13	7.2	CVE-2026-73670
sc0ttkclark--Pods Custom Content Types and Fields	The Pods - Custom Content Types and Fields plugin for WordPress is vulnerable to Privilege Escalation via Authorization Bypass in all versions up to, and including, 3.3.9. The vulnerability exists because the pods_admin AJAX router funnels every access check - including the method allowlist, nonce verification, login enforcement, and capability gate - through pods_error(), which under the JSON meta-box-loader compatibility path only writes failures to the PHP error log and returns false instead of terminating the request, rendering all guards ineffective. This makes it possible for unauthenticated attackers to escalate their privileges to Administrator or overwrite the password of any user account, including the site owner's, enabling complete site takeover, or perform another administrator action.	2026-08-15	9.8	CVE-2026-19598
SCADA-LTS--ScadaLTS	ScadaLTS 2.7.8.1 exposes a server-side method that lacks authorization checks, allowing any authenticated user (including one holding only low-privilege, read-only permissions) to execute arbitrary operating system commands on the host. Successful exploitation results in code execution in the context of the ScadaLTS server process (root), leading to full compromise of the underlying system.	2026-08-12	9.9	CVE-2026-19656
scriban--scriban	Scriban before 7.2.2 contains an access-modifier bypass vulnerability in TypedObjectAccessor that allows template code to write CLR object properties	2026-08-16	9.8	CVE-2026-73061

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	without setter-visibility checks. Attackers can modify properties with private, internal, or init-only setters, and perform mass assignment on public-setter properties, permanently altering live host objects after template rendering.			
scriban--scriban	Scriban before 7.0.0 caches TypedObjectAccessor by Type only without considering MemberFilter changes, allowing reused TemplateContext instances to expose members that should be hidden. Attackers can access filtered properties and fields by reusing a TemplateContext after tightening its MemberFilter, bypassing sandbox policies across requests or tenants.	2026-08-16	9.1	CVE-2026-74790
scriban--scriban	Scriban before 7.0.0 fails to clear the CachedTemplates dictionary when TemplateContext.Reset() is called, allowing cached templates to persist across reused contexts. Attackers can exploit request-dependent ITemplateLoader implementations to access previously authorized template content from earlier renders without triggering TemplateLoader.Load() again.	2026-08-16	8.6	CVE-2026-74791
scriban--scriban	Scriban versions from 3.0.0 through 7.2.5 contain a denial of service vulnerability in the ScriptRange.Multiply operator that bypasses LoopLimit when the left operand is a lazy sequence. Attackers can supply templates with array multiplication on lazy sequences to execute billions of uncharged iterations, pinning CPU cores and exhausting garbage collection resources even when LoopLimit is set to 1.	2026-08-16	7.5	CVE-2026-73060
scriban--scriban	Scriban versions 3.0.0 through 7.2.0 contain a denial of service vulnerability in the array multiplication operator that allocates memory without enforcing LoopLimit or overflow-safe arithmetic checks. Attackers can supply a large integer multiplier in a template to force multi-gigabyte memory allocations, causing resource exhaustion and availability degradation.	2026-08-16	7.5	CVE-2026-73062
scriban--scriban	Scriban versions 6.6.0 through 7.2.0 contain a non-enforcing ExpressionDepthLimit guard that fails to stop recursive descent parsing of deeply nested expressions. Attackers can supply templates with deeply nested parentheses, array initializers, object initializers, or unary operators to trigger an uncatchable StackOverflowException that immediately terminates the host process.	2026-08-16	7.5	CVE-2026-74783
scriban--scriban	Scriban before 7.0.0 contains an uncontrolled recursion vulnerability in the object.to_json builtin function that lacks depth limits and circular reference detection. Attackers can craft templates with self-referencing objects to trigger unbounded recursion, causing a StackOverflowException that fatally terminates the hosting .NET process.	2026-08-16	7.5	CVE-2026-74787
scriban--scriban	Scriban before 7.0.0 (affected versions <= 6.6.0) contains an uncontrolled memory allocation vulnerability in the string.pad_left and string.pad_right template functions, which perform no validation on the width parameter before delegating to .NET's String.PadLeft/PadRight. When an application exposes Scriban to untrusted template input, an attacker can supply an arbitrarily large width value (e.g., 500,000,000) to trigger ~1GB memory allocations in a single call, resulting in OutOfMemoryException and denial of service. The TemplateContext.LimitToString limit does not prevent this because it is only enforced after the string has been fully allocated.	2026-08-16	7.5	CVE-2026-74788
scriban--scriban	Scriban before 7.0.0 (affected <= 6.6.0) applies its LoopLimit constraint only to script loop statements and not to expensive iteration performed inside built-in operators and functions. As a result, a single expression such as {{ 1..1000000 array.size }} - or a memory-amplification expression such as {{ 'A' * 200000000 }} - can force large CPU or memory consumption even when LoopLimit is configured to a very small value, resulting in denial of service. Applications that render attacker-controlled templates and rely on LoopLimit for safe execution are affected.	2026-08-16	7.5	CVE-2026-74789
scriban--scriban	Scriban before 7.0.0 (affected versions <= 6.6.0) contains a stack overflow vulnerability in nested array initializer parsing. Deeply nested array initializers recurse through a path (ParseArrayInitializer â†’ ParseExpression â†’ ParseArrayInitializer) that is not covered by the ExpressionDepthLimit counter added in the fix for GHSA-wgh7-7m3c-fx25. An attacker who can supply untrusted input to Template.Parse can trigger an uncatchable StackOverflowException that immediately terminates the process, even with the default ExpressionDepthLimit enabled.	2026-08-16	7.5	CVE-2026-74792
scriban--scriban	Scriban before 6.6.0 contains an infinite recursion vulnerability in object rendering when the ObjectRecursionLimit property defaults to unlimited. Attackers can supply circular reference objects to the template context, exhausting stack space and triggering an uncatchable StackOverflowException that terminates the hosting process.	2026-08-16	7.5	CVE-2026-74794
scriban--scriban	Scriban before 6.6.0 contains an uncontrolled recursion vulnerability in its recursive-descent parser. The parser does not enforce a default expression depth	2026-08-16	7.5	CVE-2026-74795

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	limit (the ExpressionDepthLimit property in ParserOptions defaults to null/disabled), so an attacker who controls template input can supply a deeply nested template (e.g., thousands of nested parentheses or blocks) that exhausts thread stack space and raises a StackOverflowException. Because a StackOverflowException cannot be caught in .NET, this causes immediate, unrecoverable termination of the hosting process, resulting in a denial of service. Applications that process untrusted or user-supplied templates can be exploited remotely without authentication.			
scriptsbundle--Nokri	Unauthenticated Broken Access Control in Nokri <= 1.6.6 versions.	2026-08-13	9.8	CVE-2026-66691
seaweedfs--seaweedfs	SeaweedFS is a distributed storage system. Prior to 4.24, the filer registers the SeaweedIdentityAccessManagement gRPC service without mandatory authentication when jwt.filer_signing.key is unset, allowing any client that can reach the filer gRPC port to invoke CreateUser, CreateAccessKey, PutPolicy, and related IAM RPCs to mint credentials and gain S3 administrative control. This issue is fixed in versions 4.24.	2026-08-11	9.8	CVE-2026-72920
seaweedfs--seaweedfs	SeaweedFS is a distributed storage system. Prior to 4.24, VolumeServer.FetchAndWriteNeedle in weed/server/volume_grpc_remote.go fetches a caller-supplied remote endpoint through weed/remote_storage/s3/s3_storage_client.go and writes the response into a needle. The RPC performs no authentication and no target validation, allowing anyone who can reach a volume server's gRPC port to cause requests to arbitrary hosts, including loopback, link-local, RFC 1918, and cloud metadata endpoints such as 169.254.169.254, and read the response. On cloud deployments, this can disclose instance metadata and IAM credentials and reach otherwise unexposed internal services. The volume server gRPC plane is unauthenticated by default, and configuring documented JWT signing keys does not protect this RPC. This issue is fixed in version 4.24.	2026-08-11	9.3	CVE-2026-73080
seaweedfs--seaweedfs	SeaweedFS is a distributed storage system. Prior to 4.24, the weed/server/filer_server_handlers.go allowed _prefixes authorization check used strings.HasPrefix on raw path strings, so a filer JWT scoped to /tenant1 also authorized sibling paths such as /tenant1234, /tenant1-old, and /tenant1backup, enabling cross-tenant reads and writes with a valid scoped token. This issue is fixed in version 4.24.	2026-08-11	8.1	CVE-2026-72921
seerr-team--seerr	Seerr is an open-source media request and discovery manager for Jellyfin, Plex, and Emby. Prior to version 3.4.0, Seerr's ImageProxy in server/lib/imageproxy.ts uses the upstream ETag and Content-Type response headers to build a cache filename for the unauthenticated GET /avatarproxy/:jellyfinUserId route, allowing a malicious or compromised Jellyfin or Emby server, or a man-in-the-middle attacker on a plaintext media-server connection, to supply traversal sequences that path.join and fs.writeFile normalize outside the cache directory, overwrite /app/dist/index.js or other files, and execute code as the node user after a container restart. This issue is fixed in version 3.4.0.	2026-08-12	7.1	CVE-2026-73291
semaphoreui--semaphore	Semaphore UI is a web interface for managing DevOps tools. Prior to 2.18.17 and 2.19.5-beta2, repository git_url handling passes an attacker-controlled --upload-pack option to CmdGitClient.GetLastRemoteCommitHash through POST /api/project/{id}/repositories and scheduled commit-hash polling, allowing a project Manager or Owner to execute arbitrary OS commands in the Semaphore server process. This issue is fixed in versions 2.18.17 and 2.19.5-beta2.	2026-08-12	9.9	CVE-2026-73294
semaphoreui--semaphore	Semaphore UI is a web interface for managing DevOps tools. Prior to 2.18.21, the /api/users/{id}/password endpoint accepts a cross-site request using the authenticated user's semaphore session cookie without CSRF protection or current-password confirmation, allowing an unauthenticated attacker to change an administrator's or another user's password after user interaction. This issue is fixed in version 2.18.21.	2026-08-12	8.3	CVE-2026-73292
semaphoreui--semaphore	Semaphore UI is a web interface for managing DevOps tools. Prior to 2.18.19 and from 2.19.0-alpha3 until 2.19.5-beta5, ProjectMiddleware and GetProjectOrGlobalRoleBySlug allow a project manager to use POST /api/project/{id}/roles to create a custom manager role with permission bitmask 15, overriding the built-in manager permissions and granting CanUpdateProject and CanManageProjectUsers owner capabilities. This issue is fixed in versions 2.18.19 and 2.19.5-beta5.	2026-08-12	8.8	CVE-2026-73293
semaphoreui--semaphore	Semaphore versions prior to 2.18.20 contain an OS command injection (argument injection) vulnerability in the repository git_url handling that allows authenticated	2026-08-14	8.8	CVE-2026-73682

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	users holding the Manager or Owner role on any project to achieve remote code execution on the Semaphore server host. Attackers can craft a malicious git_url value using git's --upload-pack= option to inject and execute arbitrary shell commands when the server processes repository operations using the default cmd_git client.			
seriousm4x--UpSnap	UpSnap is a wake on lan web app. Versions prior to 5.4.0 have an OS command injection vulnerability in the UpSnap's device management functionality due to the presence of unsafe shell command template interpolation using the ip and the mac fields. User-controlled values can be inserted into the wake_cmd and shutdown_cmd templates and executed via /bin/sh -c (Linux) or cmd /C (Windows) without sanitization, resulting in an authenticated Remote Code Execution (RCE). A low-privileged user with permission to create or edit devices can execute arbitrary operating system commands on the UpSnap hosted server. Version 5.4.0 patches the issue.	2026-08-12	9.6	CVE-2026-49481
seriousm4x--UpSnap	UpSnap is a wake on lan web app. Versions 4.4.1 through 5.3.5 are vulnerable to a missing-authentication / privilege-escalation chain in `pb.HandlerInitSuperuser` ('backend/pb/handlers.go:249'), reachable as `POST /api/upsnap/init-superuser`. The vulnerable code lacks any authentication, setup token, IP allow-list, or rate limit and is gated only by a `totalSuperusers > 0` count check - a condition that is false on every fresh install - allowing an unauthenticated network-adjacent attacker to register the initial superuser account, receive a long-lived JWT, and pivot to root remote code execution at `backend/networking/wake.go:43` ('exec.CommandContext(ctx, "/bin/sh", "-c", wake_cmd)'). Version 5.4.0 fixes the issue.	2026-08-12	9.8	CVE-2026-49819
shabti--Frontend Admin by DynamiApps	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 3.29.9. The vulnerability exists because `ActionUser::conditions_logic()` gates the `current_user_can('edit_user', \$user_id)` authorization check behind an `is_numeric()` test, causing the check to be skipped entirely when `\$user_id` is a non-numeric string - a condition that can be induced by passing a crafted value such as `1one` through the unvalidated `item_id` parameter of the unauthenticated `wp_ajax_nopriv_frontend_admin/forms/change_form` AJAX endpoint. This makes it possible for attackers to escalate privileges to administrator by obtaining a server-signed `_acf_objects` payload carrying the non-numeric user ID, which WordPress subsequently coerces to integer 1 (the default administrator), allowing the attacker to overwrite that account's password or email address. Exploitation by unauthenticated users requires a public-facing frontend user form to be configured; in all other cases a subscriber-level account is sufficient.	2026-08-16	9.8	CVE-2026-18432
shabti--Frontend Admin by DynamiApps	The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.29.9. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level and above permissions, to reset the password of any user on the site, including administrators, leading to full account takeover and complete site compromise. Exploitation requires the attacker to hold a valid encrypted Current-User token obtained by accessing any Edit User form they are legitimately authorized to submit, which they then use as a known-plaintext base for the CBC bit-flipping forgery.	2026-08-11	8.8	CVE-2026-15606
Shamalli--Web Directory Free	Unauthenticated SQL Injection in Web Directory Free <= 1.7.13 versions.	2026-08-13	9.3	CVE-2026-28142
shepherdwind--velocity.js	Velocity.js is a JavaScript implementation of the Apache Velocity template engine. Prior to 2.1.7, the earlier fix for CVE-2026-44966 filtered constructor, __proto__, and prototype only in the #set assignment handler in src/compile/set.ts, while property-read expressions in src/compile/references.ts remained unfiltered. The getReferences() flow called getAttributes(), whose property access allowed an attacker-controlled template to traverse constructor.constructor to the JavaScript Function constructor. The #set handler validated only the assignment target and did not inspect the right-hand property-read expression, allowing arbitrary shell commands, environment-variable access, cloud-credential access, and internal-network access in the server process. This issue is fixed in version 2.1.7.	2026-08-13	9.8	CVE-2026-73649
Siemens--Parasolid V38.0	A vulnerability has been identified in Parasolid V38.0 (All versions < V38.0.235), Parasolid V38.1 (All versions < V38.1.230). The affected applications contains an out of bounds read vulnerability while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-64629

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siemens--Siemens License Server (SLS)	A vulnerability has been identified in Siemens License Server (SLS) (All versions < V5.3). The affected application is vulnerable to a path traversal vulnerability due to lack of sanitization of user input. This could allow a remote attacker to access arbitrary files on the application.	2026-08-11	7.5	CVE-2026-69109
Siemens--SIMATIC IoT2050 Advanced	A vulnerability has been identified in SIMATIC IoT2050 Advanced (6ES7647-0BA00-1YA2) (All versions < V4.3.4.1 running Industrial OS with Node-RED installed). Affected devices do not enforce authentication on the Node-RED HTTP interface, allowing unauthenticated access to programming nodes that are capable of executing system commands on the server. This could allow an unauthenticated remote attacker to create malicious flows through the HTTP interface in order to execute arbitrary code on the underlying server with maximum privileges.	2026-08-11	10	CVE-2026-58115
Siemens--Simcenter Femap	A vulnerability has been identified in Simcenter Femap (All versions < V2606), Simcenter Nastran (All versions < V2606). The affected applications contain a stack overflow vulnerability while parsing specially strings as argument for one of the application binaries. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-59086
Siemens--Simcenter Femap	A vulnerability has been identified in Simcenter Femap (All versions < V2606.0001). The affected applications contains an out of bounds read vulnerability while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-59700
Siemens--Simcenter Femap	A vulnerability has been identified in Simcenter Femap (All versions < V2606.0001). The affected applications contains an out of bounds read vulnerability while parsing specially crafted BMP files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-59701
Siemens--Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 15), Solid Edge SE2026 (All versions < V226.0 Update 7). The affected applications contains an out of bounds read vulnerability while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-50058
Siemens--Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 15), Solid Edge SE2026 (All versions < V226.0 Update 7). The affected applications contains an out of bounds write vulnerability while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-50059
Siemens--Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 15), Solid Edge SE2026 (All versions < V226.0 Update 7). The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-50060
Siemens--Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 15), Solid Edge SE2026 (All versions < V226.0 Update 7). The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted DFT files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-50061
Siemens--Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 15), Solid Edge SE2026 (All versions < V226.0 Update 7). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-50062
Siemens--Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 15), Solid Edge SE2026 (All versions < V226.0 Update 7). The affected applications contains an out of bounds read vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-50063
Siemens--Solid Edge SE2025	A vulnerability has been identified in Solid Edge SE2025 (All versions < V225.0 Update 15), Solid Edge SE2026 (All versions < V226.0 Update 7). The affected applications contains an out of bounds write vulnerability while parsing specially crafted PSM files. This could allow an attacker to execute code in the context of the current process.	2026-08-11	7.8	CVE-2026-50064
Significant-Gravitas--AutoGPT	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to 0.6.70, AutoGPT's autogpt_platform/backend/backend/api/features/integrations/router.py webhook_ingress_generic route selected get_webhook_manager(provider) from the untrusted provider URL segment without verifying webhook.provider, allowing	2026-08-11	8.2	CVE-2026-72922

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a request to /compass/webhooks/{webhook_id}/ingress to use CompassWebhookManager's inherited no-op BaseWebhooksManager.verify_signature instead of GenericWebhooksManager.verify_signature, bypass X-Webhook-Secret for a configured secret_token, and execute a generic webhook graph as its owner. This issue is fixed in version 0.6.70.			
sigstore--fulcio	Fulcio is a certificate authority for issuing code signing certificates for an OpenID Connect (OIDC) identity. Versions through 1.8.5 improperly follow cross-host redirects and attach Kubernetes ServiceAccount tokens during OIDC discovery, allowing a malicious or compromised issuer to perform blind SSRF, substitute and cache malicious JWKS keys, or disclose ServiceAccount tokens to external hosts. Version 1.8.6 blocks cross-host redirects, restricts token injection, and restricts local token loading. No known workarounds are available.	2026-08-13	8.7	CVE-2026-49478
sigstore--rekor	Rekor is a software supply chain transparency log. Starting in version 0.3.0 and prior to version 1.5.2, the `Package.Unmarshal()` function in `pkg/types/alpine/apk.go` decompresses the signature and control gzip members of an APK file into in-memory buffers without bounding the total decompressed size. The existing `max_apk_metadata_size` check (default 1MB) is only applied to individual tar entry header sizes after decompression completes, so it does not prevent a decompression bomb from consuming unbounded heap memory. An attacker can craft a gzip stream that compresses at a ~1000:1 ratio (e.g., 2MB compressed zeros → 2GB decompressed). When submitted as spec.package.content in an Alpine `ProposedEntry`, the server decompresses the full payload into memory during request processing, triggering a fatal Go runtime out-of-memory error or OS OOM-kill that cannot be caught by the server's recover() middleware. This is reachable via two unauthenticated endpoints, `POST /api/v1/log/entries (createLogEntry)` and `POST /api/v1/log/entries/retrieve (searchLogQuery)`. Both invoke `V001Entry.Canonicalize()` → `fetchExternalEntities()` → `apk.Unmarshal(packageData)`, which performs the unbounded decompression. Version 1.5.2 patches the issue. There is no effective workaround. Setting `max_request_body_size` reduces but does not eliminate exposure due to the ~1000:1 compression ratio (a 1MB body limit still allows ~1GB heap allocation). Setting `max_apk_metadata_size` has no effect on this vulnerability since the check is applied after decompression.	2026-08-13	7.5	CVE-2026-48702
silabs.com--WiseConnect	Spoofing an already bonded device can force either RS9116W or SiWx917 to re-pair/bond with a rogue device. See V1 in BLERP paper below	2026-08-13	8.8	CVE-2026-16101
silabs.com--WiseConnect	Bluetooth re-pairing with an existing device can use a lower security level. RS9116W and SiWx91x impacted. See V3 in the BLERP paper linked below.	2026-08-13	8.8	CVE-2026-19291
silabs.com--WiseConnect	Re-pairing with a legitimate device can use a lower security level than previous making brute-forcing the LTK easier. See V4 in the BLERP paper linked below.	2026-08-13	8.8	CVE-2026-19292
silabs.com--WiseConnect	SMP security request (from peripheral) does not include the maximum encryption key size supported. Using a key with less than the maximum keysize makes brute-forcing the key easier. See V6 in BLERP paper linked below.	2026-08-13	8.8	CVE-2026-19293
sixstorage--6Storage Rentals	The 6Storage Rentals plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.27.0. This is due to the six_storage_create_wp_user() AJAX handler being registered on wp_ajax_nopriv_six_storage_create_wp_user without any nonce, capability, credential, or ownership verification, while calling wp_set_current_user() and wp_set_auth_cookie() for any WordPress user resolved by the attacker-supplied email address. This makes it possible for unauthenticated attackers to log in as any existing WordPress user, including administrators, by submitting that user's email address.	2026-08-15	9.8	CVE-2026-15303
siyuan-note--siyuan	SiYuan versions <= v3.7.2 contain a SQL injection vulnerability in the backlink/mention search query (kernel/model/backlink.go), which concatenates stored block metadata (title, name, alias, anchor text) and the client-supplied keyword into a SQL MATCH/search statement while escaping only the double-quote character and not the single quote. A single quote in the client keyword (first-order, reachable by an anonymous or RoleReader user on the publish surface) or in stored document metadata (second-order) breaks out of the string literal. Because the query runs on the main read-write siyuan.db handle via a statement-stacking-capable driver, an attacker can execute arbitrary SQL, enabling cross-notebook read and write. Fixed in v3.7.4.	2026-08-14	10	CVE-2026-72811
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to validate or escape annotation fields written to disk by the setFileAnnotation endpoint. Attackers can inject malicious markup into	2026-08-15	9	CVE-2026-73041

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	annotation fields that execute as script in the PDF renderer with full Node.js access when a user opens an annotated PDF.			
siyuan-note--siyuan	SiYuan before v3.7.4 fails to properly escape database menu metadata in HTML interpolation, allowing stored values to execute script when users open group, view, or field-edit menus. Attackers can inject markup through field descriptions or names that close containing elements and execute arbitrary code via event handlers, reaching Node built-ins due to Electron's insecure configuration.	2026-08-15	9	CVE-2026-73042
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain a remote code execution vulnerability in the Template calculation operator, which renders user-authored Go templates and stores output verbatim without sanitization. Attackers can inject malicious HTML and JavaScript into template calculations that execute in the desktop client renderer with Node integration enabled, allowing arbitrary code execution when the database is opened.	2026-08-15	9	CVE-2026-73043
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to validate or escape table column width values, allowing stored cross-site scripting injection into style attributes. Attackers can inject malicious payloads through the setAttrViewColWidth API that break out of style attributes and inject event handlers on every table cell, executing arbitrary code in the Electron renderer with Node integration enabled.	2026-08-15	9	CVE-2026-73044
siyuan-note--siyuan	SiYuan before v3.7.4 improperly restricts excessive authentication attempts in the CheckAuth() middleware. The HTTP Basic Authentication branch, which guards nearly the entire /api/* surface, accepts the workspace access code (Conf.AccessAuthCode) as the Basic Auth password but never consults the CAPTCHA/lockout gate or increments the failure counter used by the cookie/session login path. This allows unauthenticated remote attackers to brute-force the admin access code with unlimited automated requests and obtain full RoleAdministrator access to the kernel. A secondary weakness exists because the access code is compared using a non-constant-time string comparison.	2026-08-15	9.8	CVE-2026-73046
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to validate or escape the color field in attribute-view select options, allowing stored cross-site scripting through eight unescaped render sites. Attackers can inject event-handler attributes by including quotation marks in the color value, executing arbitrary JavaScript when viewing databases containing the malicious select field.	2026-08-15	9	CVE-2026-73050
siyuan-note--siyuan	SiYuan before v3.7.4 stores attribute-view field names without HTML escaping and interpolates them directly into option elements via innerHTML in the sort menu. Attackers can inject markup by renaming a database field to execute arbitrary JavaScript when users open the sort menu, with Node integration enabled in the desktop client enabling code execution.	2026-08-15	9	CVE-2026-73052
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain a cross-site scripting vulnerability in the unicode2Emoji function that fails to sanitize codepoint branch output. Attackers can craft document icons with hex-encoded markup that executes in the renderer with Node integration enabled, achieving arbitrary code execution on the host system.	2026-08-15	9	CVE-2026-73053
siyuan-note--siyuan	SiYuan kernel versions before 3.7.4 contain an improper restriction of excessive authentication attempts vulnerability in the CheckAuth() middleware. The middleware accepts the API token (Conf.Api.Token) via an Authorization header (Token/Bearer) or a ?token= query parameter, and neither path is protected by the application's CAPTCHA/lockout mechanism (NeedCaptcha/WrongAuthCount). As a result, an unauthenticated remote attacker can perform unlimited automated guesses of the API token, particularly when a short or weak custom token has been configured, and upon success gains full RoleAdministrator access enabling arbitrary file operations and SQL queries.	2026-08-16	9.8	CVE-2026-73056
siyuan-note--siyuan	SiYuan before v3.7.4 fails to properly validate publish access for encrypted notebooks, treating them as publicly accessible by default. Anonymous readers can enumerate and retrieve fully decrypted document content from unlocked encrypted notebooks through the publish API without authentication or key material.	2026-08-12	8.6	CVE-2026-72789
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to mask sensitive configuration fields in the /api/system/getConf endpoint, allowing anonymous or publish-reader users to obtain the session-cookie signing key, OS username via pandoc path, and encrypted-notebook key material. Attackers can forge and tamper with session cookies to impersonate users, and on instances without access-auth codes configured, escalate to administrator privileges.	2026-08-12	8.6	CVE-2026-72793
siyuan-note--siyuan	siyuan versions before v3.7.4 expose the session cookie signing key through the /api/system/getConf endpoint to unauthenticated users in publish mode. Attackers	2026-08-12	8.6	CVE-2026-72794

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	can retrieve the CookieKey value and forge valid session cookies to impersonate users or gain administrative access.			
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to filter embedded block content by publish access in the getBlockDOMWithEmbed and getBlockDOMsWithEmbed endpoints. Attackers can request published blocks containing embed queries to read content from password-protected, hidden, or forbidden documents without authorization.	2026-08-12	8.6	CVE-2026-72795
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to properly filter related-database content in renderAttributeView, allowing anonymous readers to access Relation and Rollup cell contents from hidden or password-protected databases. Attackers can request published databases that relate to restricted databases to retrieve sensitive content, or bypass row filtering entirely when the first column is a non-block type.	2026-08-12	8.6	CVE-2026-72798
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to validate publish-password tier in getGraph and getLocalGraph endpoints, allowing anonymous readers to retrieve block-level content of password-protected documents. Attackers can call these endpoints without supplying a password to read protected document content and the complete reference topology.	2026-08-12	8.6	CVE-2026-72804
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain a second-order SQL injection vulnerability in attribute-view template columns that expose the queryBlocks function, which executes raw SQL using string substitution instead of parameterized queries. Attackers can distribute malicious SiYuan documents or packages with crafted template columns that execute arbitrary SQL on a victim's kernel when the package is imported and rendered, enabling read and write access across notebooks.	2026-08-12	8	CVE-2026-72807
siyuan-note--siyuan	SiYuan versions <= v3.7.2 (patched in v3.7.4) contain an authentication bypass vulnerability in the kernel's CheckAuth function, which grants the administrator role (RoleAdministrator) to any request whose RemoteAddr is loopback (127.0.0.1) for a specific set of endpoints (including /api/system/exit, getNetwork, getWorkspaceInfo, /assets/*, and /export/*). These localhost bypasses sit outside the access auth code gate, so they apply even when an access auth code is configured. Because the fixed-port reverse proxy forwards requests to the kernel over loopback without injecting an authentication token and does not configure trusted proxies, a request forwarded through this proxy reaches the kernel with RemoteAddr = 127.0.0.1. If the fixed-port proxy is bound to a network interface, this could allow a remote unauthenticated attacker to obtain admin access on the affected endpoints; however, per the advisory this remote forwarding behavior was established only by code inspection and was not reproduced end-to-end.	2026-08-12	8	CVE-2026-72809
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain a publish-boundary bypass vulnerability in WebSocket broadcast sessions that allows anonymous readers to receive unfiltered edits. Attackers can establish a WebSocket connection to the publish surface and passively receive real-time content events including password-protected and forbidden documents without authentication.	2026-08-14	8.6	CVE-2026-72810
siyuan-note--siyuan	SiYuan's development branch (endpoint introduced by commit 9b8e8956f, not present in v3.7.3 or master, patched in v3.7.4) contains a missing-authorization vulnerability in the /api/av/getAttributeViewSearchTarget endpoint. The route is registered with CheckAuth only and performs no authorization checks (no CheckReadOnly, no publish-access or encrypted-notebook gating). Given a database identifier taken from a published page and a keyword, an anonymous reader can query the endpoint to retrieve matching database row content, including rows that publish filters (FilterAttributeViewByPublishAccess) would otherwise withhold. No released stable version is affected.	2026-08-13	8.6	CVE-2026-73608
siyuan-note--siyuan	SiYuan versions before v3.7.4 disclose encrypted-notebook key-derivation material and wrapped data keys through unauthenticated endpoints in publish mode. Attackers can retrieve Argon2id salt, cost parameters, password verifiers, and wrapped notebook keys to perform unlimited offline master-password cracking without rate limiting.	2026-08-12	7.5	CVE-2026-72801
siyuan-note--siyuan	SiYuan before 3.7.4 contains an improper restriction of excessive authentication attempts vulnerability in the authFilePublishAccess endpoint that allows unauthenticated attackers to brute-force per-notebook publish passwords. Attackers can submit unbounded password guesses without rate limiting or CAPTCHA to gain access to password-protected published notebooks.	2026-08-15	7.5	CVE-2026-73045
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an authentication bypass vulnerability in the WebSocket endpoint caused by differential parsing of query parameters between authentication exemption and session quarantine checks. Unauthenticated attackers can craft a malicious WebSocket URI with duplicated query parameters	2026-08-15	7.5	CVE-2026-73054

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to bypass access auth code validation and receive the live kernel event stream including document identifiers, titles, and operation logs.			
smepay--SMEPay: UPI Gateway for WooCommerce	Unauthenticated Broken Access Control in SMEPay: UPI Gateway for WooCommerce <= 1.0.5 versions.	2026-08-13	7.5	CVE-2026-66461
SMEWebify--WebErpMesv2	WebErpMesv2 is a Resource Management and Manufacturing execution system Web for industry. Versions 1.19 and prior allow any self-registered user to upload arbitrary PHP files through the HR Expense scan_file parameter, leading to Remote Code Execution. Combined with open registration (no invite required) and broken role middleware (CheckUserRole silently swallows RouteNotFoundException), this chain is effectively unauthenticated RCE against any default installation. The issue is patched in commit 5c54862fa044b363fd2be03d586750e81afd6818.	2026-08-13	9.8	CVE-2026-49827
smp46--pingvin-share-x	Pingvin Share X is a secure and easy self-hosted file sharing platform. A vulnerability in versions 1.5.0 through 1.18.0 allow an attacker to bypass password verification when managing Time-based One-Time Password (TOTP) settings. The root cause is a missing `await` keyword on calls to the asynchronous `verifyPassword` method in `authTotp.service.ts` and the `authenticateUser` method in `auth.service.ts`. In JavaScript, an unawaited `Promise` is always truthy. So the logic intended to throw a `ForbiddenException` when a password is incorrect. It never executes because the expression evaluates the existence of the `Promise` object rather than its resolved boolean result. The vulnerability is fixed in version 1.18.1 by ensuring all asynchronous authentication calls are properly awaited. There are no official workarounds. If a user is locked out, an administrator must manually reset the user's TOTP status in the database.	2026-08-12	8.8	CVE-2026-49467
Snowflake--Snowflake Python APIs	Insufficient input sanitization in Snowflake Python API (`snowflake.core`) versions prior to 1.13.0 allowed confused-deputy privilege escalation through two related weaknesses: path traversal (CWE-22) via unencoded `..` identifier path segments, and HTTP parameter pollution (CWE-141) via unencoded `&`/`#`/`= characters in query string values. An attacker with access to a downstream application built on snowflake.core could exploit the path traversal by supplying `..` as an object name, causing `snowflake.core` to issue REST requests against a parent resource or exploit the parameter pollution by injecting `&`/`#`/`= into a free-form name field to override constraints on swap, clone, or rename operations - all executed under the application's privileged session. Successful exploitation requires the attacker to control an identifier or object-name string in an application built on snowflake.core that passes it to `snowflake.core` under a higher-privileged Snowflake session (e.g., an EXECUTE AS OWNER stored procedure, Streamlit app, or Native App). The fix is available in Snowflake Python API version 1.13.0, which also addresses several additional security findings. Users must manually upgrade.	2026-08-12	8.1	CVE-2026-19594
sns theme--Samex - Clean, Minimal Shop WooCommerce WordPress Theme	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sns theme Samex - Clean, Minimal Shop WooCommerce WordPress Theme and sns theme M.Anh - Fashion WooCommerce WordPress Theme allows Reflected XSS. This issue affects Samex - Clean, Minimal Shop WooCommerce WordPress Theme: from n/a through 2.5; M.Anh - Fashion WooCommerce WordPress Theme: from n/a through 1.7.	2026-08-13	7.1	CVE-2026-28154
solacewp--Solace Extra	The Solace Extra plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the import_zip() function in versions up to, and including, 1.6.0. The handler is registered on both wp_ajax_action-import-zip and wp_ajax_nopriv_action-import-zip and only verifies the 'ajax-nonce' nonce, which is emitted on every admin page via wp_localize_script (unrestricted admin_enqueue_scripts hook) and is therefore accessible to any authenticated user including Subscribers. This makes it possible for authenticated attackers, with Subscriber-level access and above, to wipe navigation menus, sidebar widgets (via update_option('sidebars_widgets', array())), all theme mods (via remove_theme_mods()), and Elementor templates, as well as trigger arbitrary demo-content imports.	2026-08-16	9.1	CVE-2026-18316
solacewp--Solace Extra	Subscriber Broken Access Control in Solace Extra <= 1.6.0 versions.	2026-08-13	7.1	CVE-2026-27535
sooperset--mcp-atlassian	MCP Atlassian is a Model Context Protocol (MCP) server for Atlassian products (Confluence and Jira). Prior to 0.22.0, confluence_upload_attachment passes its client-supplied file_path directly to open(file_path, "rb") in src/mcp_atlassian/confluence/attachments.py through upload_attachment_direct() without calling validate_safe_path. An authenticated MCP client can read any file accessible to the server process and exfiltrate it to	2026-08-12	7.7	CVE-2026-73498

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Confluence as an attachment. If an AI agent can be induced to call the tool through untrusted content, the same flaw can disclose server environment variables such as CONFLUENCE_API_TOKEN and other credentials. This issue is fixed in version 0.22.0.			
SourceCodester-- Class and Exam Timetabling System	A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0. The affected element is an unknown function of the file /edit_teacher.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	2026-08-15	7.3	CVE-2026-19899
SourceCodester-- Simple Client Management System	A security vulnerability has been detected in SourceCodester Simple Client Management System 1.0. The impacted element is an unknown function of the file /classes/Master.php?f=save_service. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	2026-08-14	7.3	CVE-2026-19825
SourceCodester-- Simple Doctors Appointment System	A weakness has been identified in SourceCodester Simple Doctors Appointment System 1.0. The affected element is an unknown function of the file /admin/ajax.php?action=set_appointment. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-10	7.3	CVE-2026-19384
SourceCodester-- Simple Student Information System	A vulnerability was found in SourceCodester Simple Student Information System. Affected by this vulnerability is an unknown functionality of the file app/admin/departments/view_department.php. Performing a manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	2026-08-13	7.3	CVE-2026-19710
SPIP--SPIP	SPIP before 4.4.18 contains a code injection vulnerability in SQLite-backed installations. The navigation menu endpoint improperly handles array-typed user input, which bypasses input sanitization and allows the value to break out of an internal quoted string context when evaluated as PHP. An authenticated attacker with at minimum editor (redacteur) privileges can submit a single crafted GET request to /ecrire/?exec=navigation to execute arbitrary OS commands in the web server process. MySQL-backed installations are not affected.	2026-08-10	8.8	CVE-2026-66738
Stanford NLP-- DSPy	DSPy 3.3.0b1 contains a file exfiltration vulnerability in the Image and Audio output field adapters that allows attackers with influence over language model outputs to read arbitrary local files by injecting a filesystem path into the url field of a parsed Image or Audio typed output. The JSONAdapter and ChatAdapter parse untrusted language model completions through parse_value into TypeAdapter validation, which triggers encode_image or encode_audio to read and base64-encode any local file path via the os.path.isfile branch in image.py and audio.py, subsequently embedding the file contents into outgoing prompt messages sent to the attacker-controlled model endpoint.	2026-08-11	8.6	CVE-2026-72742
stoatchat-- stoatchat	stoatchat before 0.15.0 fails to validate SVG viewBox dimensions in the proxy endpoint, allowing attackers to cause denial of service by memory exhaustion. Attackers can host malicious SVGs with extremely large width and height values and trigger concurrent requests to exhaust available memory across proxy replicas.	2026-08-16	7.5	CVE-2026-73057
Strategy11 Team-- Business Directory	Unauthenticated Cross Site Scripting (XSS) in Business Directory <= 6.4.25 versions.	2026-08-13	7.1	CVE-2026-28004
Strategy11-- Formidable Digital Signatures	The Formidable Digital Signatures plugin for WordPress is vulnerable to file deletion due to insufficient file path validation in the delete_file function in all versions up to, and including, 3.0.6. This makes it possible for unauthenticated attackers to delete files on the server by supplying an attacker-controlled filename in the item_meta[field_id][content] parameter alongside the delete_saved_image flag during the standard entry-creation POST flow on any form that accepts anonymous submissions.	2026-08-11	9.8	CVE-2026-16230
svg--svgo	SVGO, short for SVG Optimizer, is a Node.js library and command-line application for optimizing SVG files. From version 1.0.0 until versions 2.8.3, 3.3.4, and 4.0.2, the removeScripts plugin, named removeScriptElement in versions 1 through 3, can leave executable content in optimized SVGs because it does not remove namespaced or prefixed script elements such as <svg:script> and, in versions 3 and 4, matches JavaScript URIs case sensitively. Applications that process untrusted SVG input with this plugin enabled and serve the result can allow scripts to execute when another user opens the SVG, exposing local storage or cookies. This issue is fixed in versions 2.8.3, 3.3.4, and 4.0.2.	2026-08-13	8.2	CVE-2026-73650
Swing Music-- Swing Music	A missing authentication vulnerability in Swing Music 3.0.0 allows unauthenticated remote attackers to create arbitrary user accounts via the POST	2026-08-11	7.5	CVE-2026-72605

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/auth/profile/create endpoint. The endpoint is allowlisted from JWT verification, permitting unauthenticated account creation. An attacker can register an account and use it to access protected functionality on the server.			
Taubyte--tau	Taubyte Tau v1.1.10 contains a missing authorization vulnerability in the services/auth HTTP service that allows any authenticated user to read or permanently delete another tenant's project by supplying an arbitrary project ID to the GET and DELETE /projects/{id} endpoints. The GitHubTokenHTTPOAuth middleware only validates that a caller presents a valid GitHub OAuth token without verifying ownership or access rights to the target project, enabling attackers with any valid GitHub token to invoke bare KV-store operations such as projects.Fetch and project.Delete against any project ID to achieve cross-tenant project takeover.	2026-08-11	8.3	CVE-2026-69119
Tenable, Inc.-- Security Center	A remote code execution vulnerability exists in Tenable Security Center's report generation functionality. An authenticated, non-administrative user could exploit this issue by supplying specially crafted input that is later processed unsafely during server-side report rendering, resulting in arbitrary code execution with the privileges of the service account.	2026-08-14	9.9	CVE-2026-19626
Tenable, Inc.-- Security Center	An authenticated command injection vulnerability exists in Security Center related to file upload processing. An attacker could exploit this issue by uploading a specially crafted file, potentially resulting in arbitrary command execution on the underlying operating system.	2026-08-14	9.9	CVE-2026-19681
Tenable, Inc.-- Security Center	A command injection vulnerability exists in Security Center where a remote, unauthenticated attacker could exploit this issue to execute arbitrary commands on the underlying operating system with the privileges of the service account.	2026-08-14	9.9	CVE-2026-19682
Tenable, Inc.-- Security Center	A privilege escalation vulnerability exists in Tenable Security Center that allows a user with "Security Manager" role and "manage user" permission on a single group to modify users belonging to other groups. This bypasses the intended access control restrictions and enables unauthorized cross-group user management.	2026-08-14	8.1	CVE-2026-19629
Tenable, Inc.-- Security Center	A local privilege escalation vulnerability exists in Security Center. An attacker with write access to a specific configuration file could achieve arbitrary code execution with elevated privileges, without requiring further user or victim interaction.	2026-08-14	8.8	CVE-2026-19635
Tenable, Inc.-- Security Center	An input validation vulnerability exists in Security Center's file upload handling, where insufficient sanitization of uploaded filenames could contribute to a downstream command injection issue.	2026-08-14	8.8	CVE-2026-19679
Tenable, Inc.-- Security Center	A command injection vulnerability exists in Tenable Security Center. An authenticated administrator could modify application configuration values to achieve arbitrary command execution on the underlying operating system when specific backend operations are triggered.	2026-08-14	7.2	CVE-2026-19628
Tenable, Inc.-- Security Center	A SQL injection vulnerability exists in Security Center that could allow an attacker to access unauthorized data from the application's database.	2026-08-14	7.1	CVE-2026-19680
Tencent--APIJSON	A SQL injection vulnerability in Tencent APIJSON through 8.1.8 allows unauthenticated remote attackers to bypass per-table access control and read arbitrary database tables via the Map-form @having operator.	2026-08-10	9.8	CVE-2026-72565
Tenda--AC10	A security vulnerability has been detected in Tenda AC10 16.03.10.09_multi_TDE01. This vulnerability affects the function R7WebSecurityHandler of the component httpd. The manipulation leads to improper authentication. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	2026-08-16	9.8	CVE-2026-19924
Tenda--AC12	A vulnerability was determined in Tenda AC12 15.03.06.23_multi_TD01. This vulnerability affects the function formSetRebootTimer of the file /goform/SetSysAutoRebootCfg of the component httpd web management interface. This manipulation of the argument rebootTime causes buffer overflow. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-14	8.8	CVE-2026-19821
Tenda--AC1206	A vulnerability was found in Tenda AC1206 15.03.06.23_multi_TD01. This affects the function set_device_name of the file /goform/SetOnlineDevName of the component httpd web management interface. The manipulation of the argument devName results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	2026-08-14	8.8	CVE-2026-19788
Tenda--AC1206	A vulnerability was determined in Tenda AC1206 15.03.06.23_multi_TD01. This vulnerability affects the function set_wl_guest_iplist of the file /goform/WifiGuestSet of the component httpd web management interface. This manipulation of the argument shareSpeed causes stack-based buffer overflow.	2026-08-14	8.8	CVE-2026-19789

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.			
Tenda--CH	A flaw has been found in Tenda CH, CP and TX3 V21.x/V22.x/V25.x/V26.x/V27.x. Affected by this issue is some unknown functionality of the component SSH. Executing a manipulation can lead to use of hard-coded password. It is possible to launch the attack remotely. The attack requires a high level of complexity. The exploitation is known to be difficult. The exploit has been published and may be used.	2026-08-13	8.1	CVE-2026-19750
Tenda--CH7	A weakness has been identified in Tenda CH7, CH7G, CH10, CP3, CP3 Pro, CP7, TC3B14C, TC3B15C, TC3T14C and TC3T15C up to 20260625. This impacts the function CAtE::HandleCmd of the file Kylin of the component ATE Module. This manipulation causes command injection. The attack is possible to be carried out remotely.	2026-08-13	9.8	CVE-2026-19747
Tenda--G0	A vulnerability was identified in Tenda G0 up to 20260625. This issue affects the function formSetPortMirror of the file /goform/module of the component httpd Web Management Interface. Such manipulation of the argument portMirrorMirroredPorts leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used.	2026-08-14	8.8	CVE-2026-19790
Tenda--G0	A weakness has been identified in Tenda G0 up to 20260625. The affected element is the function addStaticRoute of the file /goform/module of the component httpd web management interface. Executing a manipulation of the argument staticRouteNet can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2026-08-14	8.8	CVE-2026-19791
Tenda--G0	A security flaw has been discovered in Tenda G0 up to 20260625. Impacted is the function setPortMapping of the file /goform/module of the component httpd web management interface. Performing a manipulation of the argument portMappingServer/porMappingtInternal/portMappingExternal results in buffer overflow. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	2026-08-14	8.8	CVE-2026-19792
Tenda--W20E	A vulnerability was identified in Tenda W20E 15.11.0.6(1068_1546_841)_CN_TDC. This issue affects the function IstAdd of the file /goform/editQos of the component QoS Edit. Such manipulation of the argument qosListConnectedNum leads to stack-based buffer overflow. The attack may be launched remotely. The exploit is publicly available and might be used.	2026-08-14	8.8	CVE-2026-19822
Tenda--W20E	A security flaw has been discovered in Tenda W20E 15.11.0.6(1068_1546_841)_CN_TDC. Impacted is the function formQOSRuleDel of the file /goform/delQos of the component QoS Rule Deletion. Performing a manipulation of the argument qosIndex results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	2026-08-14	8.8	CVE-2026-19823
Tenda--W20E	A weakness has been identified in Tenda W20E 15.11.0.6(1068_1546_841)_CN_TDC. The affected element is the function ipMacBindListStore of the file /goform/addIpMacBind. Executing a manipulation of the argument IPMacBindRule can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-14	8.8	CVE-2026-19824
The NetBSD Foundation--NetBSD	NetBSD's hdaudio(4) driver in sys/dev/hdaudio/hdaudio.c contains a missing access control vulnerability that allows unprivileged local attackers to invoke the HDAUDIO_FGRP_SETCONFIG ioctl without elevated permissions by exploiting the absence of an access check on /dev/hdaudioN device nodes. Attackers can repeatedly issue HDAUDIO_FGRP_SETCONFIG from one thread while keeping DMA and IRQs live from a second thread to trigger a use-after-free race condition in hdaifg_detach() between stream_stop() and stream_disestablish(), where a latched DMA interrupt dereferences a freed callback pointer, resulting in outcomes ranging from audio-subsystem denial of service and kernel panic to potential local kernel privilege escalation.	2026-08-12	7	CVE-2026-53996
themefic--Hydra Booking	Unauthenticated Broken Access Control in Hydra Booking <= 1.2.2 versions.	2026-08-13	7.3	CVE-2026-28188
themefic--Travelfic Toolkit	Subscriber Broken Access Control in Travelfic Toolkit <= 1.5.1 versions.	2026-08-13	8.1	CVE-2026-28186
Themeisle--WP Full Stripe Free	Unauthenticated Cross Site Scripting (XSS) in WP Full Stripe Free <= 8.5.0 versions.	2026-08-13	7.1	CVE-2026-61960

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
themetechmount--TrueBooker Appointment Booking and Scheduler System	The TrueBooker plugin for WordPress is vulnerable to Account Takeover in all versions up to, and including, 1.2.6. This is due to the add_front_user_update() AJAX handler being registered for unauthenticated users and accepting an arbitrary truebooker_wp_user_id value, which is passed directly to wp_update_user() without verifying authentication or ownership. This makes it possible for unauthenticated attackers to change any WordPress user account email address, including an administrator, by submitting the target user ID and an attacker-controlled email address. An attacker can then use the native WordPress password reset flow to receive the reset link at the attacker-controlled email address and take over the account.	2026-08-15	9.8	CVE-2026-16142
ThimPress--RealPress	Unauthenticated SQL Injection in RealPress <= 1.1.2 versions.	2026-08-13	9.3	CVE-2026-66458
TOTOLINK--A800R	A security flaw has been discovered in TOTOLINK A800R 4.1.2cu.5137_B20200730. The impacted element is the function setIpQosRules of the file /cgi-bin/cstecgi.cgi of the component firewall.so. The manipulation of the argument Comment results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	2026-08-14	8.8	CVE-2026-19811
TOTOLINK--A800R	A weakness has been identified in TOTOLINK A800R 4.1.2cu.5137_B20200730. This affects the function UploadCustomModule of the file /cgi-bin/cstecgi.cgi of the component product.so. This manipulation of the argument File causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-14	8.8	CVE-2026-19812
TOTOLINK--A800R	A security vulnerability has been detected in TOTOLINK A800R 4.1.2cu.5137_B20200730. This impacts the function setMacFilterRules of the file /cgi-bin/cstecgi.cgi of the component firewall.so. Such manipulation of the argument Comment leads to stack-based buffer overflow. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2026-08-14	8.8	CVE-2026-19813
TOTOLINK--A800R	A vulnerability was detected in TOTOLINK A800R 4.1.2cu.5137_B20200730. Affected is the function setMacQos of the file /cgi-bin/cstecgi.cgi of the component firewall.so. Performing a manipulation of the argument macAddress results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2026-08-14	8.8	CVE-2026-19814
TOTOLINK--A800R	A flaw has been found in TOTOLINK A800R 4.1.2cu.5137_B20200730. Affected by this vulnerability is the function setParentalRules of the file /cgi-bin/cstecgi.cgi of the component firewall.so. Executing a manipulation of the argument urlKeyword can lead to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been published and may be used.	2026-08-14	8.8	CVE-2026-19815
TOTOLINK--A800R	A vulnerability was found in TOTOLINK A800R 4.1.2cu.5137_B20200730. The impacted element is the function setRadvdCfg of the file /cgi-bin/cstecgi.cgi of the component ipv6.so. Performing a manipulation of the argument radvdinterfacename results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	2026-08-14	8.8	CVE-2026-19844
TOTOLINK--A800R	A vulnerability was determined in TOTOLINK A800R 4.1.2cu.5137_B20200730. This affects the function setStaticDhcpConfig of the file /cgi-bin/cstecgi.cgi of the component lan.so. Executing a manipulation of the argument Comment can lead to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-14	8.8	CVE-2026-19845
TOTOLINK--A800R	A vulnerability was identified in TOTOLINK A800R 4.1.2cu.5137_B20200730. This impacts the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi of the component firewall.so. The manipulation of the argument url leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit is publicly available and might be used.	2026-08-14	8.8	CVE-2026-19846
TOTOLINK--A800R	A security flaw has been discovered in TOTOLINK A800R 4.1.2cu.5137_B20200730. Affected is the function setWiFiWpsConfig of the file /cgi-bin/cstecgi.cgi of the component wps.so. The manipulation of the argument pin results in stack-based buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-08-14	8.8	CVE-2026-19847
triggerdotdev--trigger.dev	Trigger.dev is a platform for building and deploying fully managed AI agents and workflows. Prior to 4.5.6, POST /api/v1/deployments/:deploymentId/background-workers calls CreateDeploymentBackgroundWorkerServiceV4.call() in apps/webapp/app/v3/services/createDeploymentBackgroundWorkerV4.server.ts, where workerDeployment.findFirst() selects a deployment by friendlyId without an environmentId predicate. A caller with a valid API key for one project can submit another project's deployment identifier, link an attacker-owned background	2026-08-13	9.9	CVE-2026-73656

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	worker to the victim deployment, and move the victim deployment from BUILDING to DEPLOYING. This issue is fixed in version 4.5.6.			
triggerdotdev--trigger.dev	Trigger.dev is a platform for building and deploying fully managed AI agents and workflows. From 3.3.8 until 4.5.6, the PUT /api/v1/runs/:runId/metadata endpoint passes attacker-controlled operation.key values to new JSONHeroPath(operation.key).set(newMetadata, value) in packages/core/src/v3/runMetadata/operations.ts without rejecting dangerous constructor and prototype path segments. A caller with a normal environment API key can pollute Object.prototype in the shared webapp process, corrupting Prisma queries and Prometheus labels, breaking other tenants' worker authentication, and causing a process-wide denial of service. This issue is fixed in version 4.5.6.	2026-08-13	8.5	CVE-2026-73654
triggerdotdev--trigger.dev	Trigger.dev is a platform for building and deploying fully managed AI agents and workflows. From 4.4.2 until 4.5.0-rc.5, Aws4FetchClient.buildUrl() and Aws4FetchClient.presign() in apps/webapp/app/v3/objectStoreClient.server.ts assign user-controlled packet keys to URL.pathname, while apps/webapp/app/routes/api.v1.packets.\$ts accepts params["*"] without rejecting dot segments and uses findResource: async () => 1 without per-resource ownership validation. WHATWG path normalization collapses .. segments before signing, allowing a caller with a valid environment API key to obtain presigned URLs for another tenant's object-store keys and read or overwrite task payloads. This issue is fixed in version 4.5.0-rc.5.	2026-08-13	8.2	CVE-2026-73658
triggerdotdev--trigger.dev	Trigger.dev is the open-source platform for building AI workflows in TypeScript. From 4.4.2 until 4.5.0, the packet presign routes in apps/webapp/app/routes/api.v1.packets.\$ts pass a caller-controlled filename through resolveStoreProtocolForPacketPresign to generatePresignedUrl and generatePresignedRequest in apps/webapp/app/v3/objectStore.server.ts, allowing .. traversal to escape the packets/<projectRef>/<env>/ object-store prefix and enabling a project API key to read or overwrite another organization's offloaded task payloads and outputs on multi-organization self-hosted instances. This issue is fixed in version 4.5.0.	2026-08-13	8.1	CVE-2026-73659
triggerdotdev--trigger.dev	Trigger.dev is a platform for building and deploying fully managed AI agents and workflows. Prior to 4.5.2, addGoogleStrategy() in apps/webapp/app/services/googleAuth.server.ts passes a Google profile email to findOrCreateGoogleUser() in apps/webapp/app/models/user.server.ts without requiring Google's email_verified assertion. When existingEmailUser && !existingUser is true, the flow writes the new Google authIdentifier into the existing email-matched account and returns that user object, allowing an attacker-controlled Google profile with an unverified matching email to take over the account. This issue is fixed in version 4.5.2.	2026-08-13	7.4	CVE-2026-73655
truelockmc--streambert	Streambert is a cross-platform Electron Desktop App to stream and download video content. Versions prior to 2.5.0 improperly validate executable paths supplied to the run-download IPC handler, allowing a compromised renderer process to execute arbitrary local binaries with the application's privileges. Version 2.5.0 contains a patch.	2026-08-11	10	CVE-2026-48056
twentyhq--twenty	Twenty is an open-source CRM (customer relationship management) platform. Prior to 2.15.0, Twenty allowed a workspace administrator with the DATA_MODEL permission to supply settings.asExpression for the system TS_VECTOR field searchVector through PATCH /rest/metadata/fields/:id or the updateOneField GraphQL mutation, causing buildSqlColumnDefinition in packages/twenty-server/src/engine/twenty-orm/workspace-schema-manager/utis/build-sql-column-definition.util.ts to concatenate unescaped input into GENERATED ALWAYS AS (...) and execute arbitrary PostgreSQL statements as the application database user. This issue is fixed in version 2.15.0.	2026-08-11	9.1	CVE-2026-73069
usmannasir--cyberpanel	CyberPanel before 3.0.0 contains a hard-coded JWT secret vulnerability in the WebTerminal FastAPI SSH service that allows unauthenticated remote attackers to forge valid authentication tokens and obtain an interactive root shell via WebSocket on port 8888. Attackers can craft a forged JWT signed with the hardcoded secret value, specifying ssh_user=root, to authenticate to the terminal service without any valid credentials and receive a root shell.	2026-08-13	9.8	CVE-2026-67614
usmannasir--cyberpanel	CyberPanel 2.4.3, fixed in commit eca0c3c, contains an authenticated remote code execution vulnerability in the remote backup feature that allows authenticated attackers to gain root-level SSH access by supplying a malicious remote server address. Attackers can exploit the unverified SSH public key retrieval process to	2026-08-10	8.8	CVE-2026-71965

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	write an attacker-controlled public key directly to /root/.ssh/authorized_keys, granting persistent root access to the host system.			
usmannasir--cyberpanel	CyberPanel 2.4.3, fixed in commit eca0c3c, contains an authenticated command injection vulnerability in the remote backup transfer feature that allows authenticated attackers to execute arbitrary OS commands by controlling a remote server's API response. Attackers can inject malicious commands through a crafted directory name in the remote server's API response, which bypasses security middleware validation and is passed unsanitized to the OS command execution function.	2026-08-10	8.8	CVE-2026-71966
vcita--Online Booking & Scheduling Calendar for WordPress by vcita	The Online Booking & Scheduling Calendar for WordPress by vcita plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'business_id' parameter in all versions up to, and including, 4.6.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-15	7.2	CVE-2026-14433
vitest-dev--vitest	Vitest is a testing framework powered by Vite. Prior to versions 3.2.7, 4.1.10, and 5.0.0-beta.6, Browser Mode provider commands including upload, takeScreenshot, screenshotMatcher, stopChunkTrace, deleteTracing, and annotateTraces accept browser-supplied file paths without enforcing the allowWrite permission gate or confining paths to the project root. A client that can reach the Browser Mode API can read arbitrary local files, create or overwrite image and trace files, or delete files accessible to the Vitest process even when allowWrite is false. This issue is fixed in versions 3.2.7, 4.1.10, and 5.0.0-beta.6.	2026-08-13	9.4	CVE-2026-73653
Weaver Network Co., Ltd.--E-cology 8.0	Weaver (Fanwei) E-cology 8.0 contains a SQL injection vulnerability in the SignatureDownload servlet that allows unauthenticated remote attackers to read arbitrary files by injecting a UNION SELECT payload into the markId GET parameter, which is concatenated unsanitized into a SQL query. Attackers can control the markPath value returned by the query to supply an attacker-controlled filesystem path, causing the servlet to read and stream back arbitrary files accessible to the application server process, including sensitive configuration files containing database credentials. Disclosure materials indicate that this vulnerability has been remediated, but it's unclear which version resolved the issue. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-18 (UTC).	2026-08-11	7.5	CVE-2016-20097
Weaver Network Co., Ltd.--E-cology 9.0	Weaver (Fanwei) E-cology 8.0 and 9.0 contains a SQL injection vulnerability in the HrmCareerApplyPerView.jsp endpoint that allows unauthenticated remote attackers to extract arbitrary data from the backend database by manipulating the id GET parameter. Attackers can send a single crafted GET request with UNION-based injection payloads through the unsanitized id parameter to retrieve arbitrary data from the Microsoft SQL Server backend. This vulnerability is potentially remediated in software version 10.53 or 10.54. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-10-18 (UTC).	2026-08-11	7.5	CVE-2022-50997
WebCodingPlace--Real Estate Manager Pro	The Real Estate Manager Pro plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 12.8.6. This is due to improper capability handling in the allow_attachment_actions() function, which can treat a target user ID as a media attachment ID during user capability checks. This makes it possible for authenticated attackers, with Subscriber-level access and above, to edit an administrator account and escalate their privileges to Administrator when the targeted user ID matches the ID of an existing media attachment.	2026-08-15	7.5	CVE-2026-15142
Webilia Inc.--Listdom	Unauthenticated SQL Injection in Listdom <= 5.6.0 versions.	2026-08-13	9.3	CVE-2026-61969
weDevs--StoreGrowth: Smart Sales Booster for WooCommerce BOGO, Upsells, Direct Checkout, Quick View, Side Cart	Unauthenticated Broken Access Control in StoreGrowth: Smart Sales Booster for WooCommerce BOGO, Upsells, Direct Checkout, Quick View, Side Cart <= 2.1.1 versions.	2026-08-13	7.5	CVE-2026-66466
Wei-Shaw--sub2api	Sub2API is an AI API gateway platform designed to distribute and manage API quotas from AI product subscriptions. From 0.1.135, to 0.1.168, platform API keys issued to tenants are exchanged for upstream requests made with shared provider accounts (ChatGPT/Codex OAuth, OpenAI platform keys, or an operator-configured base URL) that belong to the operator, not to the caller. The `POST	2026-08-11	8.5	CVE-2026-73079

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/responses/*subpath` wildcard routes spliced the client-supplied subpath into the upstream URL with no validation. This lets an authenticated tenant relay requests to arbitrary upstream endpoints using pooled account credentials via a path traversal. This vulnerability is fixed in 0.1.169.			
Welcart--Welcart e-Commerce	Unauthenticated Cross Site Scripting (XSS) in Welcart e-Commerce <= 2.11.31 versions.	2026-08-13	7.1	CVE-2026-27539
wg-easy--wg-easy	An OS command injection vulnerability in wg-easy 15.3.0 allows users with the clients.create permission to execute arbitrary commands as root by injecting newline-delimited WireGuard PostUp directives into the client name field. The client name is written to the WireGuard configuration file without neutralizing newline characters, allowing injection of arbitrary directives that are executed by wg-quick with root privileges. An attacker with clients.create permission achieves root code execution on the host.	2026-08-11	9.9	CVE-2026-72603
Win Men International--Travel Agency Management System	Travel Agency Management System developed by Win Men International has a SQL Injection vulnerability. Unauthenticated remote attackers can inject arbitrary SQL commands to read, modify, and delete database contents.	2026-08-11	9.8	CVE-2026-19425
Wishlist Member--Wishlist Member	The Wishlist Member plugin for WordPress is vulnerable to Account Takeover via Insufficient Verification of Data Authenticity in versions up to and including 3.34.1. This is due to the wpm_register() function validating the registration cookie only against the GET reg parameter while accepting the POST mergewith and POST wpm_id parameters without verifying that the mergewith user ID references a temporary or incomplete registrant that is bound to the current registration transaction. This makes it possible for unauthenticated attackers to take over any existing WordPress account - including administrator accounts - by supplying an arbitrary user's numeric ID as the mergewith value, which causes wp_update_user() to overwrite the target account's username (additionally written via a direct \$wpdb UPDATE), password, email address, first name, and last name with attacker-controlled values, while WordPress password and email change notification emails are explicitly suppressed. When wpm_id references a non-existent membership level, no role key is added to the update payload, causing wp_update_user() to preserve the target user's existing role - including administrator - making full privilege escalation a direct consequence of the takeover.	2026-08-14	9.8	CVE-2026-12949
wolfsoftwaresyste msLtd--WolfStack	WolfStack before 25.9.2 contains a hard-coded cluster-authentication secret compiled into every build and published as a constant in src/auth/mod.rs, allowing remote unauthenticated attackers to bypass authentication by supplying this value in the X-WolfStack-Secret header to the require_auth() gate without any session, API key, or user account. Attackers can reach an affected node's management port to enumerate all Docker and LXC containers on the host and execute arbitrary commands as root inside any container via the POST /api/containers/{runtime}/{id}/exec endpoint.	2026-08-12	9.8	CVE-2026-73519
WoompaLoompa--Bitcoin Lightning Payment Gateway for WooCommerce (via CLINK)	Unauthenticated Broken Access Control in Bitcoin Lightning Payment Gateway for WooCommerce (via CLINK) <= 1.0.7 versions.	2026-08-13	7.5	CVE-2026-66431
wp-buy--Visitors Traffic Real Time Statistics	Unauthenticated Cross Site Scripting (XSS) in Visitors Traffic Real Time Statistics <= 8.11 versions.	2026-08-13	7.1	CVE-2026-28175
wpdevteam--Templately Elementor & Gutenberg Template Library: 6500+ Free & Pro Ready Templates And Cloud!	The Templately - Elementor & Gutenberg Template Library: 6500+ Free & Pro Ready Templates And Cloud! plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 3.7.1 via the fetch_remote_file function. This is due to a filename validation/destination mismatch in fetch_remote_file, where file type validation is performed against the attacker-controlled Content-Disposition filename rather than the URL-path-derived destination filename. This makes it possible for authenticated attackers, with contributor-level access and above, to execute code on the server. A GIF+PHP polyglot file passes wp_check_filetype_and_ext validation as image/gif via the Content-Disposition filename, while the actual destination path is written with a .php extension derived from the URL path, bypassing the unfiltered_upload capability gate entirely. The affected endpoints are reachable at this privilege level because Templately's entire REST API - including the cloud import endpoints used	2026-08-15	8.8	CVE-2026-18438

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in this attack (/templately/v1/clouds/upload and /templately/v1/insert) - is authorized only by a current_user_can('delete_posts') check, with no administrator or manage_options capability requirement. The same permission gate also allows a contributor to overwrite the site's global Templately cloud connection via the /templately/v1/login endpoint with global_signin set to true. A complete remediation should both correct fetch_remote_file to validate the file type against the actual destination filename rather than the Content-Disposition header (and avoid deriving the write path from the request URL), and restrict state-changing Templately REST routes to an appropriate administrator-level capability.			
WPDirectoryKit--WP Directory Kit	Unauthenticated SQL Injection in WP Directory Kit <= 1.5.4 versions.	2026-08-13	9.3	CVE-2026-28001
WPDirectoryKit--WP Directory Kit	Unauthenticated SQL Injection in WP Directory Kit <= 1.5.4 versions.	2026-08-13	7.5	CVE-2026-27538
wplegalpages--WPLP Cookie Consent Cookie Banner & Consent Management for GDPR, CCPA & Google Consent Mode	The Cookie Banner for GDPR / CCPA - WPLP Cookie Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'regionArray' parameter in all versions up to, and including, 4.3.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Successful exploitation requires that the site administrator has enabled the 'Support Google Consent Mode (GCM)' setting, which is disabled by default. Additionally, the AJAX handler performs no nonce or capability check, allowing any authenticated user including those with Subscriber-level access to overwrite the affected plugin setting.	2026-08-15	7.2	CVE-2026-13360
wpmanageninja--Fluent Forms Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder	The Fluent Forms - Customizable Contact Forms, Survey, Quiz, & Conversational Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Notification Smartcode Values in all versions up to, and including, 6.2.11 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute in the browser of an administrator (or any user with the Fluent Forms entry-viewing capability) when they view the form's entry Submission Logs in the WordPress admin dashboard. Exploitation requires that a site administrator or Fluent Forms manager has configured an email notification whose subject or static (direct) Send To value references an attacker-influenced Smartcode such as an input_password field value, a cookie value, or submission.response.	2026-08-13	7.2	CVE-2026-18146
WPManageNinja--Fluent Forms Pro	Fluent Forms Pro 6.2.7 contains an embedded malicious code vulnerability introduced via a tampered plugin build served through a decommissioned update server. The tampered build introduced a rogue PHP file (libs/class-license-sync.php), loaded via a require_once directive added to fluentformpro.php, that established a backdoor REST API endpoint, dropped persistent PHP files in mu-plugins and uploads directories, installed a passwordless administrator account, and registered scheduled tasks that survived plugin removal.	2026-08-13	9.8	CVE-2026-73532
WPManageNinja--Ninja Tables Pro	Ninja Tables Pro 5.2.11 contains an embedded malicious code vulnerability introduced via a tampered plugin build served through a decommissioned update server. The tampered build introduced a rogue PHP file (app/Library/updater/NinjaTableDataSync.php) that established a backdoor REST API endpoint, dropped persistent PHP files in mu-plugins and uploads directories, installed a passwordless administrator account, and registered scheduled tasks that survived plugin removal.	2026-08-13	9.8	CVE-2026-73533
wproyal--Royal Addons for Elementor Addons and Templates Kit for Elementor	The Royal Elementor Addons plugin for WordPress is vulnerable to Server-Side Request Forgery in versions up to, and including, 1.7.1064 via the Form Builder widget's 'webhook_url' setting. The widget's render() method persists the attacker-controlled URL into the wpr_webhook_url_{widget_id} option on every render (including a Contributor previewing their own draft), and the wpr_form_builder_webhook AJAX handler - registered for both authenticated and unauthenticated callers - reads that option and dispatches the outbound request via the non-safe wp_remote_post(), with no host allowlist, no scheme restriction, and no private/loopback IP filter (the plugin's existing wpr_is_blocked_remote_host / wpr_is_private_or_local_ip helpers are not called on this path). This makes it possible for authenticated attackers, with Contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2026-08-16	8.8	CVE-2026-17123
wptravelengine--WP Travel Engine	The WP Travel Engine - Tour Booking Plugin - Tour Operator Software plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including,	2026-08-16	7.5	CVE-2026-17087

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Tour Booking Plugin Tour Operator Software	6.8.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to view private booking billing details - including the victim customer's first name, last name, email address, street address, city, and phone number - rendered as default values in checkout form fields by binding an arbitrary booking ID to the attacker's session. The only access control on the endpoint is a frontend nonce that is publicly emitted to all visitors via the wteL10n global on trip pages, meaning it provides CSRF protection only and does not restrict unauthenticated access.			
WWBN--AVideo	AVideo contains an unauthenticated arbitrary file write vulnerability in the aVideoEncoderChunk.json.php endpoint that allows remote attackers to write up to 4 GB of arbitrary content to the server filesystem via HTTP PUT requests without authentication. Attackers can exhaust disk space causing denial of service, poison the video encoding pipeline, or chain this with local file inclusion to achieve remote code execution.	2026-08-11	9.1	CVE-2026-72748
WWBN--AVideo	AVideo fails to sanitize the phone field during user registration, allowing unauthenticated attackers to inject malicious JavaScript that persists in the database. When administrators visit the users management page, the unsanitized phone value is rendered via innerHTML, executing the injected script in the admin's browser session.	2026-08-11	7.2	CVE-2026-72747
xerrors--Yuxi	Yuxi is a large-model-based intelligent knowledge base and knowledge graph agent development platform. Prior to version 0.6.2, the project's authentication mechanism contains a flaw. In affected versions, the system does not sufficiently validate the identity token in the Authorization header - only performing a validity check. This allows an administrator token generated in another deployment instance or local testing environment to be used to access the backend management interfaces of a different affected instance. An attacker who obtains or constructs an acceptable administrator Authorization token may bypass normal login authentication and gain administrator privileges. This vulnerability could allow an attacker to access system configurations, invoke backend management APIs, create administrator accounts, and ultimately take over the system backend. This issue has been fixed in version 0.6.2. Before upgrading, users are advised to implement the following temporary measures: Set the environment variable 'JWT_SECRET_KEY' to a non-default value, and configure a unique, sufficiently strong JWT/authentication key for each deployment instance; and/or avoid exposing backend management interfaces directly to the public network.	2026-08-12	9.4	CVE-2026-50561
xwiki--xwiki-platform	XWiki Platform is a generic wiki platform. XWiki discovered that the patch for GHSA-5cf8-rr8-8hjm was insufficient. Starting with version 6.2.1 and prior to versions 18.0.0RC1, 17.10.13, 17.4.9 and 16.10.17, with slightly modified parameters to the 'LiveTableResults', it is still possible to discover password hashes one bit at a time, so with 768 requests, the full password salt and hash can be retrieved of a user. The check for password (and email properties) has been adjusted in XWiki 18.0.0RC1, 17.10.13, 17.4.9 and 16.10.17. As a workaround, the patch can be applied manually to the wiki page 'XWiki.LiveTableResultsMacros'.	2026-08-10	7.5	CVE-2026-48048
YesWiki--yeswiki	YesWiki is a wiki system written in PHP. Prior to version 4.6.4, an unauthenticated SQL injection in the Bazar form-import path ('FormManager::create()') allows any unauthenticated visitor of a default YesWiki install to inject arbitrary SQL into an 'INSERT' statement and read the full database, including 'yeswiki_users.password' hashes. Version 4.6.4 fixes the issue.	2026-08-11	9.8	CVE-2026-46670
ymw0407--auth-fetch-mcp	auth-fetch-mcp is an MCP server that lets AI assistants fetch content from authenticated web pages. Version 3.0.1 implements SSRF protection in 'assertSafeUrl()' ('src/security.ts') to block requests to private and loopback addresses. However, the 'isPrivateV6()' function fails to detect IPv4-mapped IPv6 loopback addresses in their hex-normalized form. When an attacker supplies a URL such as 'http://[::ffff:127.0.0.1]:PORT/', the Node.js WHATWG URL parser silently normalizes the host to '[::ffff:7f00:1]'. Because 'net.isIPv4('7f00:1')' returns 'false', the private-IP check is bypassed and the URL is passed to the browser or HTTP client, allowing the MCP tool to reach loopback services that are supposed to be blocked. The issue is exploitable under default configuration without any special environment variable. Version 3.0.1 patches the issue.	2026-08-13	7.4	CVE-2026-49857
yonifre--Maspik Spam blacklist	Unauthenticated Cross Site Scripting (XSS) in Maspik - Spam blacklist <= 2.9.1 versions.	2026-08-13	7.1	CVE-2026-28003
Zalktis Programmas (SIA "Zalktis	SQL injection in the Zalktis accounting application via trading-partner-controlled text fields in received electronic invoices. When importing a received e-invoice (UBL/PEPPOL) or an e-commerce export, Zalktis concatenates partner-controlled	2026-08-13	8.8	CVE-2026-59109

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Programmas")-- Zalktis	values directly into SQL statement text using string concatenation, with neither parameterised queries nor escaping. The application's own escaping helper, <code>Dazadi.sql_txt()</code> , is not invoked on these code paths, so a party that sends an invoice can break out of the string literal and alter the query logic. This issue affects Zalktis: before 2026.1.586 and before 2026.2.592.			
ZAYTECH--Smart Online Order for Clover	Unauthenticated Cross Site Scripting (XSS) in Smart Online Order for Clover <= 1.6.1 versions.	2026-08-13	7.1	CVE-2026-66700
zephyrproject--zephyr	The user-space system-call verifier <code>z_vrfy_z_log_msg_static_create()</code> in <code>subsys/logging/log_msg.c</code> was a pure pass-through: it forwarded the caller-supplied source, desc, package, and data arguments directly to the kernel-mode implementation <code>z_impl_z_log_msg_static_create()</code> without performing any of the mandatory <code>K_SYSCALL_*</code> checks. Because <code>z_log_msg_static_create()</code> is declared <code>__syscall</code> , under <code>CONFIG_USERSPACE</code> any unprivileged user-mode thread can invoke it directly with fully attacker-controlled arguments. The kernel-mode handler dereferences each of these untrusted values: <code>frontend_runtime_filtering()</code> reads through the source pointer as a struct <code>log_source_dynamic_data</code> , <code>cbprintf_package_copy()</code> reads <code>desc.package_len</code> bytes from the package pointer, and <code>z_log_msg_finalize()</code> performs a <code>memcpy()</code> of <code>desc.data_len</code> bytes from the data pointer. With no verification, a user thread can supply arbitrary kernel addresses and arbitrary lengths, and the kernel will read from them. The impact is a kernel-mode denial of service (the kernel faults dereferencing an attacker-chosen pointer) and, where a log backend output is observable to the attacker, disclosure of arbitrary kernel memory copied into the emitted log message - a confidentiality breach across the user/kernel boundary that the userspace sandbox is meant to enforce. The reads do not corrupt kernel memory, so there is no out-of-bounds write primitive. The fix adds the required validation to the verifier: it bounds <code>desc.package_len</code> against <code>Z_LOG_MSG_MAX_PACKAGE</code> , rejects non-NULL/length mismatches, and applies <code>K_SYSCALL_MEMORY_READ()</code> to package, data, and (when runtime filtering with a frontend is enabled) source, so any out-of-bounds or kernel pointer now raises <code>K_OOPS</code> instead of being honored.	2026-08-14	8.4	CVE-2026-12364
zephyrproject--zephyr	Zephyr's dynamic kernel-object disposal path <code>unref_check()</code> in <code>kernel/userspace/userspace.c</code> frees an object's storage (<code>k_free(dyn->data)</code>) once its reference count reaches zero, after running a per-object-type cleanup. The cleanup switch handled only <code>K_OBJ_MSGQ</code> and <code>K_OBJ_STACK</code> ; there was no <code>K_OBJ_TIMER</code> case. A dynamically-allocated, initialized, and armed <code>k_timer</code> keeps its embedded struct <code>timeout</code> dnode linked in the global timeout queue (<code>_timeout_q</code>), so freeing the timer storage without cancelling the timeout leaves a dangling node in that queue. When the timer next expires, the timeout machinery walks <code>_timeout_q</code> and invokes <code>z_timer_expiration_handler()</code> on the freed node, dereferencing and writing freed (and reusable) kernel heap in kernel/ISR context. This is a deterministic use-after-free that does not depend on SMP: the queued node is simply never unlinked at free time. The disposal is reachable from an unprivileged user thread under <code>CONFIG_USERSPACE + CONFIG_DYNAMIC_OBJECTS</code> : a thread that holds the last permission on such a timer drops it via the <code>k_object_release()</code> syscall (or by exiting, through <code>k_thread_perms_all_clear()</code>), and can arm the timer itself via the <code>k_timer_start()</code> syscall. The free and the expiration handler run at kernel privilege while the actor is a user thread, so the bug is a sandbox-escape memory-corruption primitive usable for privilege escalation. The fix adds <code>k_timer_cleanup()</code> (cancel the timeout and wait for any in-flight handler) and calls it for <code>K_OBJ_TIMER</code> before freeing.	2026-08-14	8.8	CVE-2026-12366
zephyrproject--zephyr	<code>tls_opt_dtls_peer_connection_id_value_get()</code> in <code>subsys/net/lib/sockets/sockets_tls.c</code> , which handles <code>getsockopt(SOL_TLS, TLS_DTLS_PEER_CID_VALUE)</code> , passed the caller-supplied <code>optval</code> directly to <code>mbedtls_ssl_get_peer_cid()</code> without verifying the buffer was at least <code>MBEDTLS_SSL_CID_OUT_LEN_MAX</code> (default 32) bytes. <code>mbedtls_ssl_get_peer_cid()</code> copies the peer-negotiated DTLS Connection ID (length <code>1..MBEDTLS_SSL_CID_OUT_LEN_MAX</code>) into that buffer without a destination-size parameter, so a caller-supplied <code>optlen</code> smaller than the CID causes a write of up to 31 bytes past the buffer end. In <code>CONFIG_USERSPACE</code> builds the <code>getsockopt</code> syscall verifier (<code>z_vrfy_zsock_getsockopt</code>) bounce-buffers the user's <code>optval</code> into a kernel allocation of exactly <code>optlen</code> bytes (<code>k_usermode_alloc_from_copy -> z_thread_malloc</code>), so an unprivileged user thread that passes a small <code>optlen</code> on a connected DTLS socket with Connection ID enabled induces a kernel-heap buffer overflow, with the overflowing content being the remote peer's CID. The defect	2026-08-10	8.4	CVE-2026-8718

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	requires CONFIG_MBEDTLS_SSL_DTLS_CONNECTION_ID, an established DTLS session with a negotiated peer CID, and (for the kernel-crossing case) CONFIG_USERSPACE. Introduced when the TLS_DTLS_CID option was added (v3.5.0). The fix rejects callers whose optlen is below MBEDTLS_SSL_CID_OUT_LEN_MAX with -EINVAL.			
zephyrproject--zephyr	The UpdateHub firmware-update agent's probe handler (z_impl_updatehub_probe() in subsys/mgmt/updatehub/updatehub.c) parses the JSON metadata returned by the update server into a fixed two-level nested-array struct. After parsing it validates only the outer array length (objects_len != 2) and then dereferences objects[1].objects[0].objects.sha256sum via strlen() without checking that the inner object array of element [1] is non-empty. The metadata is attacker-influenceable network input: the agent fetches it over CoAP from the configured UpdateHub server during its routine OTA probe. A malicious or compromised update server (or, when DTLS is disabled, a network man-in-the-middle) can return a response whose second outer object array is empty. Because the parse target is zero-initialised, the corresponding objects[1].objects[0].objects.sha256sum pointer is NULL, and the subsequent strlen() dereferences address zero. The same defect exists in both the 'any boards' and 'some boards' metadata layouts. The resulting CPU fault is fatal under Zephyr's default error handling, halting or resetting the device, so the flaw is a remotely triggerable denial of service. Impact is limited to availability; it is a read from NULL with no out-of-bounds write, memory corruption, or information disclosure. The fix rejects metadata whose inner object array is empty before any dereference, on both layouts.	2026-08-10	7.5	CVE-2026-11810
zephyrproject--zephyr	The userspace syscall verifiers z_vrfy_zsock_sendmsg() and z_vrfy_zsock_recvmsg() in subsys/net/lib/sockets/sockets.c snapshot the caller-supplied struct net_msghdr into a kernel-side copy with k_usermode_from_copy(), but then re-read the still-live user struct for subsequent decisions. The kernel iovec shadow buffer is sized from one read of msg->msg_iovlen, while the population loop is bounded by a second, live read of the same field. Because msg points into ordinary user memory, a cooperating second thread in the same memory domain can inflate msg->msg_iovlen in the window between the sizing read and the loop test (a classic double-fetch / TOCTOU). The population loop then iterates past the number of net_iovec slots actually allocated, writing attacker-influenced iov_base/iov_len values beyond the end of the kernel-heap shadow buffer. The recvmsg verifier has the same defect on both its inbound and result write-back loops. The code is reachable from an unprivileged user thread whenever CONFIG_USERSPACE is enabled and the zsock_sendmsg/zsock_recvmsg syscalls are available. A successful race corrupts kernel-managed heap memory across the user-to-kernel privilege boundary, yielding a local privilege-escalation primitive or, at minimum, a kernel-fault denial of service. The fix copies the header once and derives every size, bound, and gate from the snapshot, copying each iovec entry atomically so its base and length can no longer be raced apart.	2026-08-12	7.8	CVE-2026-12234
Zimbra--Collaboration	A remote code execution vulnerability exists in Zimbra Collaboration (ZCS) before 10.1.20 when the optional zimbra-snmp package is installed and SNMP notifications are enabled. Due to improper sanitization of untrusted input during SNMP notification processing, an unauthenticated attacker can send specially crafted SMTP requests that may result in execution of arbitrary operating system commands as the Zimbra user.	2026-08-13	8.9	CVE-2026-73570
Zohocorp--ManageEngine M365 Manager Plus	Zohocorp ManageEngine M365 Manager Plus and M365 Security Plus versions below 4820 are affected to Authenticated Path Traversal vulnerability in Exchange Online backup module.	2026-08-11	8.5	CVE-2026-16053
Zohocorp--ManageEngine Password Manager Pro	Zohocorp ManageEngine Password Manager Pro versions before 13232 and ManageEngine PAM360 versions before 8552 are vulnerable to authenticated SQL injection.	2026-08-13	8.8	CVE-2026-11840
Zohocorp--ManageEngine Password Manager Pro	Zohocorp ManageEngine Password Manager Pro versions before 13232 and PAM360 versions before 8551 are vulnerable to an authentication bypass vulnerability due to improper SAML validation.	2026-08-13	8.8	CVE-2026-12263
zohocorp--manageengine_ddi_central	An authentication bypass in ManageEngine DDI Central's password-reset workflow allows account takeover.	2026-08-11	9.8	CVE-2026-12571

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ZoneMinder-- ZoneMinder	A remote code execution vulnerability in ZoneMinder 1.39.17 allows any authenticated user to execute OS commands by exploiting a broken permission check in the Filter class. The canEdit() and canDelete() methods invoke nonexistent methods on the ZM\User class, causing PHP __call() to return a truthy value that bypasses the permission check for all users. Any authenticated user can trigger filter-based OS command execution regardless of their assigned role.	2026-08-11	8.8	CVE-2026-72556
Zoom Communications-- Zoom Clients	Missing bounds check in the annotator function of Zoom Clients allows buffer over-write, which may allow a meeting participant to achieve remote code execution of another participant via network access.	2026-08-11	8.3	CVE-2026-53413
Zoom Communications-- Zoom Clients	Use after Free in the annotator function of Zoom Clients may allow a meeting participant to achieve remote code execution of another participant via network access.	2026-08-11	8.3	CVE-2026-53415
Zoom Communications-- Zoom VDI	Path traversal in Zoom VDI Client and Plugins may allow an authenticated user to conduct information disclosure via local access.	2026-08-11	7.1	CVE-2026-53416
Zyxel Networks-- WAH7601	Improper neutralization of special elements used in an OS command ('OS command injection') vulnerability in Zyxel Networks WAH7601 allows OS Command Injection. This issue affects WAH7601: through 20072026.	2026-08-10	9.8	CVE-2026-13206
Zyxel Networks-- WAH7601	Insufficiently Protected Credentials vulnerability in Zyxel Networks WAH7601 allows Retrieve Embedded Sensitive Data. This issue affects WAH7601: through 20072026.	2026-08-10	8.2	CVE-2026-12984
Zyxel Networks-- WAH7601	Use of Hard-coded Credentials vulnerability in Zyxel Networks WAH7601 allows Read Sensitive Constants Within an Executable. This issue affects WAH7601: through 20.07.2026.	2026-08-10	7.3	CVE-2026-6374
101gen-- Automation Web Platform Notifications and OTP for WooCommerce, Advanced Country Code	The Automation Web Platform - Notifications and OTP for WooCommerce, Advanced Country Code plugin for WordPress is vulnerable to Authentication Bypass in versions up to, and including, 4.8.6. This is due to the handle_email_otp_return() function returning the secret magic login token in the response to a publicly accessible OTP request, rather than only delivering it to the user's email address. This makes it possible for unauthenticated attackers to log in as any user on the site, including administrators, if they know that user's email address.	2026-08-21	9.8	CVE-2026-77264
10Web--Form Maker by 10Web	Unauthenticated Cross Site Scripting (XSS) in Form Maker by 10Web <= 1.15.46 versions.	2026-08-20	7.1	CVE-2026-66616
10Web--Slider by 10Web	Unauthenticated Cross Site Request Forgery (CSRF) in Slider by 10Web <= 1.2.62 versions.	2026-08-18	7.4	CVE-2026-66635
2100 Technology-- Official Document Management System	Official Document Management System developed by 2100 Technology has an Arbitrary File Upload vulnerability, allowing authenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	2026-08-17	8.8	CVE-2026-74845
4xmen--xshop	xShop is an open-source shop developed in Laravel. An Unrestricted File Upload vulnerability in xShop version 3.0.3 allows an authenticated administrator to upload executable files (e.g., .php). By uploading a specially crafted php file, an attacker can achieve Remote Code Execution (RCE) on the server, leading to a full system compromise. Version 3.0.4 fixes the issue.	2026-08-21	9.1	CVE-2026-49849
AeternaLabsHQ-- PullMD	A vulnerability has been found in AeternaLabsHQ PullMD 3.2.0. This impacts an unknown function of the file /api of the component REST API Endpoint. The manipulation of the argument url leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.3.0 will fix this issue. The identifier of the patch is 96448894cc93ccecb0bdcbf263a9d25390a8455e. Upgrading the affected component is advised.	2026-08-20	7.3	CVE-2026-76795
Agno AGI--Agno	Agno's PythonTools in libs/agno/agno/tools/python.py contains a path traversal vulnerability that allows attackers to read, write, or execute arbitrary files by supplying parent-directory traversal sequences in the file_name argument passed to read_file, save_to_file, or run_python_file tool actions. Attackers can inject traversal sequences such as '.././.././.././etc/passwd' through direct tool invocation or via prompt injection embedded in agent-processed content to escape the intended base_dir boundary and achieve arbitrary file read, arbitrary file write, or arbitrary Python code execution within the process user's authority.	2026-08-19	8.8	CVE-2026-76832
AKIN Software Computer Import Export Industry and Trade Ltd.--	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in AKIN Software Computer Import Export Industry and Trade Ltd. AKINSOFT Wolvox9 ERP / KontrolPanel.exe allows Path Traversal. This issue affects AKINSOFT Wolvox9 ERP / KontrolPanel.exe: from s26.02.17 before 26.02.22.	2026-08-18	7.5	CVE-2026-15585

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AKINSOFT Wolvox9 ERP / KontrolPanel.exe				
Amazon Ion-- Amazon Ion Java	Uncontrolled memory allocation in the binary Ion stream cursor in Amazon ion-java before 1.12.0 might allow remote actors to cause a denial of service via a crafted Ion binary document containing a declared-length field that causes excessive heap preallocation. To remediate this issue, users should upgrade to version 1.12.0.	2026-08-18	7.5	CVE-2026-75935
Amazon Ion-- Amazon Ion Java	Improper handling of highly compressed data in the GZIP auto-decompression handler in Amazon ion-java before 1.12.0 might allow remote actors to cause a denial of service via a crafted compressed Ion document that expands to an arbitrarily large size upon decompression. To remediate this issue, users should upgrade to version 1.12.0 and configure withGzipDecompressionEnabled(false) and/or set an explicit withMaximumBufferSize() when parsing untrusted input.	2026-08-18	7.5	CVE-2026-75936
amoffat--sh	sh provides Python process launching. Prior to 2.2.4, the _uid option in sh.py performs an incomplete privilege drop on Linux and Unix-like systems. When sh runs from an elevated process and launches a command with _uid set to an unprivileged user, the child changes its UID but can retain the parent process's supplementary groups because the privilege-drop sequence does not fully establish the target user's UID, primary GID, and supplementary groups. The child can therefore retain access to files or resources granted to privileged groups such as root, docker, disk, shadow, or sudo, violating the expected _uid privilege boundary. This issue is fixed in version 2.2.4.	2026-08-18	7.9	CVE-2026-54552
Anders Norn-- Chaplin	Unauthenticated Broken Access Control in Chaplin <= 2.6.8 versions.	2026-08-20	7.5	CVE-2026-74021
Anders Norn--Koji	Unauthenticated Broken Access Control in Koji <= 2.2.1 versions.	2026-08-20	7.5	CVE-2026-74020
andialbrecht-- sqlparse	sqlparse is a non-validating SQL parser module for Python. Prior to 0.6.0, SQL_REGEX in sqlparse/keywords.py and the per-position loop in sqlparse/lexer.py repeatedly scan unmatched dollar-quoted literal and multiline-comment delimiters, causing quadratic CPU consumption through sqlparse.parse(), sqlparse.format(), and sqlparse.split(). This issue is fixed in version 0.6.0.	2026-08-17	7.5	CVE-2026-59893
apify--apify-mcp-server	The Apify MCP server enables AI agents to extract data from websites using ready-made scrapers, crawlers, and automation tools available on the Apify Store. Prior to 0.10.11, getActorMCPServerURL in src/mcp/actors.ts concatenates the trusted Actor standby URL with the attacker-controlled webServerMcpPath from an Actor definition without verifying the resulting origin, allowing a malicious Actor publisher to use a userinfo-style authority value to redirect connectMCPClient to a third-party host. The call-actor, fetch-actor-details, and actor-mcp tool-loading paths pass this URL to transports in src/mcp/client.ts that attach the victim Authorization bearer token, exposing the Apify API token and enabling access to Actors, stored data, and billable compute. A victim must invoke or inspect the attacker-controlled Actor. This issue is fixed in version 0.10.11.	2026-08-18	8.1	CVE-2026-50143
ArcadeData-- arcadedb	ArcadeDB before 26.8.1 fails to bind the authenticated principal on the gRPC transaction executor thread in beginTransaction, allowing authenticated readers to execute JavaScript commands without scripting authorization checks. Attackers can execute executeCommand with a transaction ID to run unrestricted JavaScript that creates server-wide administrator accounts.	2026-08-18	9.9	CVE-2026-75843
ArcadeData-- arcadedb	ArcadeDB server (com.arcadedb:arcadedb-server) in versions 26.7.3 and earlier fails to propagate the authenticated principal to asynchronous command worker threads. When an HTTP command is submitted with awaitResponse:false, it executes on an async worker whose DatabaseContext has no bound user, causing the scripting authorization gate to become a no-op. A user with only read access to a single database can submit an asynchronous JavaScript (language=js) command via the /api/v1/command endpoint to run code with unrestricted host access (e.g., database.getSecurity().createUser) and create a server-wide administrator, escalating to full administrative control. Fixed in 26.8.1.	2026-08-18	9.9	CVE-2026-75851
ArcadeData-- arcadedb	ArcadeDB versions before 26.8.1 fail to enforce SASL authentication on data commands in the MongoDB wire-protocol plugin. Unauthenticated attackers can issue insert, find, update, delete, and create commands against any database by connecting to port 27017 without credentials.	2026-08-18	9.8	CVE-2026-75852
ArcadeData-- arcadedb	ArcadeDB versions before 26.8.1 contain a missing authentication vulnerability in the Redis wire-protocol plugin that allows unauthenticated attackers to read, write, and delete data. Attackers can connect to the Redis port and execute	2026-08-18	9.8	CVE-2026-75854

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary commands against any database on the server without providing credentials, bypassing all security gates.			
ArcadeData--arcadedb	ArcadeDB's Gremlin wire-protocol plugin (com.arcadedb:arcadedb-gremlin) in versions <= 26.7.3 enforces authentication (SASL PLAIN) but performs no authorization: it never checks database access permissions (canAccessToDatabase) and never binds the authenticated principal into the engine. As a result, any valid server credential - even one provisioned for zero or one unrelated database - can read, write, and drop data in any database on the server by selecting a target database via a traversal-source alias, completely bypassing the engine's per-type/read-only/UPDATE_SCHEMA ACLs. The issue is fixed in version 26.8.1.	2026-08-18	8.8	CVE-2026-75853
ArcadeData--arcadedb	ArcadeDB versions before 26.8.1 fail to sanitize database names in the POST /api/v1/server endpoint's create database and drop database commands, allowing authenticated root users to write and delete arbitrary files outside the configured database directory. Attackers can supply database names containing ../ sequences to create databases at arbitrary filesystem paths or recursively delete directories the server process can access.	2026-08-18	8.7	CVE-2026-75855
ArcadeData--arcadedb	ArcadeDB before 26.8.1 (arcadedb-gremlin, affected <= 26.7.3) contains a remote code execution vulnerability in its Gremlin query engine. Although the engine defaults to the documented-secure java (gremlin-lang) engine, ArcadeGremlin.executeStatement() silently falls back to the insecure Groovy engine whenever a request carries any query parameter and the query does not parse as gremlin-lang. An authenticated user with any database role, including a read-only reader, can submit a parameterized Gremlin query to trigger the Groovy fallback and execute arbitrary operating system commands as the ArcadeDB server process user.	2026-08-19	8.8	CVE-2026-76224
ArcadeData--arcadedb	ArcadeDB before 26.8.1 contains an arbitrary file read vulnerability in the GraalVM JavaScript sandbox allowlist enforcement, which uses unescaped regular expressions to validate package names. Attackers with trigger creation privileges can use Java.type() to access java.util.zip.ZipFile or java.util.jar.JarFile classes and read arbitrary files on the host system as the ArcadeDB server process.	2026-08-18	7.5	CVE-2026-75840
ArcadeData--arcadedb	ArcadeDB versions before 26.8.1 contain an arbitrary file read vulnerability in the OpenCypher LOAD CSV FROM clause that allows authenticated users to read local files. Attackers with read query privileges can use the file:// protocol in LOAD CSV statements to access arbitrary files with server process privileges, exfiltrating sensitive data directly in query responses.	2026-08-18	7.7	CVE-2026-75842
ArcadeData--arcadedb	ArcadeDB versions before 26.8.1 contain a server-side request forgery vulnerability in the IMPORT DATABASE command where the security validator resolves and checks hostnames but the subsequent connection re-resolves the raw URL and follows redirects. Authenticated attackers can bypass the validator using DNS rebinding or HTTP redirects to access cloud metadata endpoints, internal services, or read arbitrary local files on default installations.	2026-08-18	7.1	CVE-2026-75844
ArcadeData--arcadedb	ArcadeDB before 26.8.1 (affected versions <= 26.7.3) contains a missing authorization vulnerability in the DELETE FUNCTION SQL statement. DeleteFunctionStatement.executeSimple unregisters and persists deletion of a server-side function without any checkPermissionsOnDatabase (UPDATE_SCHEMA) check. Any user with database access can execute DELETE FUNCTION via the command API (POST /api/v1/command/{db}) to permanently remove any registered server-side function, including security-relevant logic, impacting integrity and availability.	2026-08-18	7.1	CVE-2026-75846
ArcadeData--arcadedb	ArcadeDB (com.arcadedb) versions 26.7.3 and earlier fail to enforce the UPDATE_SCHEMA permission check when a DEFINE FUNCTION statement targets an already-existing function library. A user with only database access can add or overwrite SQL or Cypher functions in an existing library and persist the change, enabling tampering with admin-defined function logic. The issue is fixed in 26.8.1. (JavaScript functions still trigger the UPDATE_SECURITY check and are not affected.)	2026-08-19	7.1	CVE-2026-76223
ArcadeData--arcadedb	ArcadeDB before 26.8.1 contains a server-side request forgery vulnerability in the OpenCypher LOAD CSV implementation that fails to validate HTTP/HTTPS URLs. Authenticated attackers can craft LOAD CSV queries pointing to internal network addresses or cloud metadata endpoints to make the ArcadeDB server fetch and return sensitive data from restricted services.	2026-08-19	7.7	CVE-2026-76225
AresIT--WP Compress	Unauthenticated Remote Code Execution (RCE) in WP Compress < 7.20.01 versions.	2026-08-18	10	CVE-2026-73343
Autopay--Autopay	Unauthenticated Cross Site Scripting (XSS) in Autopay <= 5.0.0 versions.	2026-08-18	7.1	CVE-2026-73338

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
averta--Depicter Slider	Unauthenticated SQL Injection in Depicter Slider <= 4.8.0 versions.	2026-08-18	7.5	CVE-2026-66622
AWS--Amazon OpenSearch Service	Improper input validation in the Time Series Visual Builder (TSVB) plugin in OpenSearch Dashboards allows an authenticated remote user to execute arbitrary code on the server via a crafted JSON payload to the metrics visualization API endpoint. This issue is a form of prototype pollution that enables remote code execution. To remediate this issue, users should upgrade to OpenSearch Dashboards 3.8 or later.	2026-08-20	8.8	CVE-2026-18420
AWS--Amazon OpenSearch Service	Improper input validation in the dashboards-observability plugin in OpenSearch Dashboards allows a remote authenticated user with write permissions to OpenSearch Dashboards saved objects to execute arbitrary JavaScript in the context of other users' browser sessions by uploading a saved asset with arbitrary web content.	2026-08-21	8.7	CVE-2026-77811
AWS--Athena Federated Query Neptune Connector	In the Neptune connector, a user with access to Neptune through Athena Federated Query could gain access to properties in the Lambda supplying the compute for the connector. To remediate this issue, users should upgrade to aws-athena-query-federation v2026.30.1 or later.	2026-08-21	9.9	CVE-2026-77810
axew3--WP w3all phpBB	Subscriber SQL Injection in WP w3all phpBB <= 3.0.5 versions.	2026-08-20	8.5	CVE-2026-73998
baserproject--basercms	baserCMS before 5.3.0 contains a SQL injection vulnerability in BcDatabaseService.php that allows authenticated administrators to inject attacker-controlled table names and configuration values directly into SQL statements across sequence update, CSV export, and table management operations. Attackers can chain a backup restore code injection flaw, where PHP code outside class definitions in schema files executes unconditionally upon loading, to plant malicious table names and trigger error-based SQL injection that retrieves database version, schema contents, and arbitrary data from the PostgreSQL backend.	2026-08-20	7.2	CVE-2026-76635
bastillion-io--Bastillion	Bastillion fails to properly validate request URI paths in its controller dispatcher, allowing unauthenticated attackers to bypass authentication filters by prefixing requests with arbitrary path segments. Attackers can access administrative controllers to read user listings, create manager accounts, and register managed systems, gaining control over SSH access to the managed fleet.	2026-08-18	9.8	CVE-2026-75627
Baylan Measuring Instruments Industry and Trade Inc.--Baylan Smart Meter Management Application (BMS)	Missing authentication for critical function vulnerability in Baylan Measuring Instruments Industry and Trade Inc. Baylan Smart Meter Management Application (BMS) allows Authentication Bypass. This issue affects Baylan Smart Meter Management Application (BMS): before v1.1.10.142.	2026-08-20	9.8	CVE-2026-15706
BelledonneCommunications--bcg729	Belledonne Communications bcg729 through 1.1.2 contains an out-of-bounds read vulnerability in the decodeSIDframe() function in src/cng.c that allows unauthenticated network-adjacent attackers to trigger a heap read beyond buffer boundaries by sending a zero-length comfort-noise RTP payload. A zero-length payload causes an integer underflow in the uint8_t filter order calculation, which wraps to 255 and is clamped to 10, causing the function to unconditionally read 11 bytes from a zero-byte buffer, resulting in media process termination or silent consumption of adjacent heap memory as reflection coefficients.	2026-08-17	7.5	CVE-2026-71980
bigbluebutton--bigbluebutton	BigBlueButton is an open-source virtual classroom. Prior to 3.0.23, BigBlueButton allowed authenticated moderators to inject SQL through the meetingId and userId values used by refreshBreakoutRoomsVisibleForUsers in akka-bbb-apps/src/main/scala/org/bigbluebutton/core/db/BreakoutRoomUserDAO.scala. The method interpolated those values into breakout room visibility queries, allowing arbitrary SQL execution against the application database. This issue is fixed in version 3.0.23.	2026-08-20	8.5	CVE-2026-46682
bigbluebutton--bigbluebutton	BigBlueButton is an open-source virtual classroom. Prior to 3.0.23, BigBlueButton exposed /bigbluebutton/api/handleJoinExistingUser through bigbluebutton-web/grails-app/controllers/org/bigbluebutton/web/controllers/ApiController.groovy. A requester able to supply an existingUserId for an active participant could reuse that participant's session and impersonate the participant in the same meeting because handleJoinExistingUser was a routable controller action rather than a private helper. This issue is fixed in version 3.0.23.	2026-08-20	7.1	CVE-2026-46355

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bluewave-labs--Checkmate	Checkmate is an open-source, self-hosted tool designed to track and monitor server hardware, uptime, response times, and incidents in real-time with beautiful visualizations. Prior to 3.9.1, the public POST /api/v1/auth/register route in server/src/api/routes/authRoutes.ts passes multipart profileImage uploads through in-memory Multer parsing before registration validation, without file-size, file-count, or MIME-type limits in server/src/api/middleware/upload.ts. An unauthenticated attacker can submit concurrent oversized files that are buffered before invalid registration or invite-token checks reject the request, exhausting memory and crashing or destabilizing the backend. This issue is fixed in version 3.9.1.	2026-08-21	7.5	CVE-2026-55241
bluewave-labs--Checkmate	Checkmate is an open-source, self-hosted tool designed to track and monitor server hardware, uptime, response times, and incidents in real-time with beautiful visualizations. From 3.3.0 until 3.9.2, enabling the global showURL setting causes the unauthenticated GET /api/v1/status-page/:url endpoint to return complete monitor objects from server/src/controllers/statusPageController.ts. The response includes the secret field used by HttpProvider.ts as an HTTP Authorization credential, even though BaseStatusPage.tsx does not display that value, allowing visitors to extract credentials from the JSON response and use them against monitored services. This issue is fixed in version 3.9.2.	2026-08-21	7.5	CVE-2026-71862
Brainstorm Force--OttoKit	Unauthenticated Server Side Request Forgery (SSRF) in OttoKit <= 1.1.35 versions.	2026-08-18	7.2	CVE-2026-32553
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.19, the PostgreSQL datasource connector in packages/server/src/integrations/postgres.ts interpolates the user-controlled schema configuration field into a SET search_path statement without escaping embedded double quotes, allowing an authenticated administrator who saves or tests the datasource to execute arbitrary SQL through the simple query protocol. This issue is fixed in version 3.39.19.	2026-08-17	8.4	CVE-2026-64657
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.40.0, packages/backend-core/src/utis/outboundFetch.ts pinned a validated address through a Node agent, but the REST integration used getDispatcher from packages/backend-core/src/utis/fetch.ts, causing undici to ignore that agent and resolve the hostname again. A builder could use DNS rebinding to make packages/server/src/integrations/rest.ts connect to an internal address after a public address passed validation, with full response access and arbitrary REST methods. The fix adds createPinnedLookup support to the undici dispatcher and passes the validated address to custom fetch implementations. This issue is fixed in version 3.40.0.	2026-08-17	8.5	CVE-2026-73410
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.41.3, POST /api/attachments/:datasourceId/url in packages/server/src/api/routes/static.ts and packages/server/src/api/controllers/static/index.ts allows an authenticated published-app user with the BASIC role to supply attacker-controlled bucket and key values and obtain signedUrl and publicUrl values backed by stored S3 datasource credentials. This issue is fixed in version 3.41.3.	2026-08-17	7.1	CVE-2026-54356
buildwps--PPWP Password Protect Pages	The PPWP - Password Protect Pages plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.9.18 via deserialization of untrusted input from the 'post_protection_roles' vulnerable parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	2026-08-22	8.8	CVE-2026-0551
Canonical--accountsservice	An Ubuntu-specific patch to AccountsService before 23.13.9-8ubuntu7 only partially drops privileges before launching language helper scripts. It changes the effective UID/GID to the target user but leaves the real UID as 0 (root). A shell spawned by a helper script inherits ruid=0 and may reset its effective UID to root, enabling local privilege escalation.	2026-08-20	7.8	CVE-2026-61897
Canonical--accountsservice	The Ubuntu-specific language helper scripts (save-to-pam-env, update-langlist) shipped with accountsservice before 23.13.9-8ubuntu7 treat the user-controlled LANGUAGE entry in ~/.pam_environment as trusted input. The value is interpolated unescaped into a GNU sed replacement expression, allowing an attacker to inject a sed 'e' flag and arbitrary shell commands that execute with the	2026-08-20	7.8	CVE-2026-61898

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileges of the AccountsService helper process (real UID 0) via the SetLanguage D-Bus method.			
celabshq--libcrux-ecdh	libcrux-ecdh and libcrux-ed25519 before 0.0.6, and libcrux-psq before 0.0.7, contain cryptographic implementation bugs. libcrux-ecdh did not properly check length and clamping during X25519 secret validation (and had a broken clamping check for imported X25519 secret keys); libcrux-ed25519 performed a duplicated clamping step during key generation; and libcrux-psq panicked instead of propagating an AEADError. These were fixed in the respective patched releases.	2026-08-19	7.5	CVE-2026-76234
centrifugal--centrifugo	Centrifugo is an open-source scalable real-time messaging server. Prior to 6.9.0, Centrifugo copies the client-controlled protocol.ConnectRequest.headers map through OnClientConnecting in internal/client/handler.go, ConnectEvent.Headers, and SetEmulatedHeadersToContext. The requestHeaders path in internal/proxy/http.go, the requestMetadata path in internal/proxy/grpc.go, and the Consume path in internal/unigrpc/grpc.go can forward an allowlisted value as a trusted backend header or metadata value. A remote client can spoof a header such as x-trusted-user for connect, refresh, subscribe, publish, RPC, and related proxy calls when the backend relies on that header for authentication or authorization. The unidirectional gRPC transport has no transport-level HTTP header that can override the emulated value. This issue is fixed in version 6.9.0.	2026-08-20	9.1	CVE-2026-71485
Centuran Consulting--OTRS Community Edition	OTRS Community Edition contains an authenticated OS command injection vulnerability in the PGP encryption module that allows administrators to execute arbitrary operating-system commands by supplying crafted values for the PGP binary path and command options. Administrator-supplied configuration values are concatenated without sanitization into a shell command, enabling arbitrary command execution as the web server process user during normal ticket operations after the malicious configuration is deployed.	2026-08-20	7.2	CVE-2026-53804
cesanta--mongoose	Mongoose is an embedded web server and network library. Prior to 7.22, a remote unauthenticated attacker can exploit an HTTP/1.0 reverse-proxy deployment by sending a request with Transfer-Encoding: chunked and conflicting framing. The http_cb() function in src/http.c tests hm.proto.len with an impossible greater-than-eight condition even though mg_http_parse() requires an eight-byte protocol string, so is_http_1_0 is never set. Mongoose consequently processes chunked encoding that an HTTP/1.0 proxy can ignore, enabling request smuggling and unauthorized access or state changes. This issue is fixed in version 7.22.	2026-08-20	9.1	CVE-2026-73256
cesanta--mongoose	Mongoose is an embedded web server and network library. Priro to version 7.22, a remote unauthenticated attacker can send an HTTP request containing both Content-Length and Transfer-Encoding: chunked. The cl_count and te_count checks in the mg_http_parse() and http_cb() paths in src/http.c accept both headers and prioritize chunked encoding, while a Content-Length-preferring reverse proxy can use a different request boundary. This CL.TE desynchronization can inject requests that access or modify resources in another user context. This issue is fixed in version 7.22.	2026-08-20	9.1	CVE-2026-73257
cgaugue--@cgaugue/yaml	@cgaugue/yaml npm package contains an arbitrary code execution vulnerability that allows attackers to execute arbitrary JavaScript by embedding a custom !js YAML tag whose construct callback unconditionally calls eval() on attacker-supplied string values during document parsing. Any application parsing untrusted YAML input with this library exposes full Node.js runtime authority, including environment variable access, filesystem read/write, network access, and subprocess execution, with no safe-mode alternative or opt-out mechanism available.	2026-08-20	7.8	CVE-2026-76833
chenhg5--cc-connect	A vulnerability was found in chenhg5 cc-connect up to 1.4.1. Affected by this vulnerability is the function Authenticate of the file core/webhook.go. The manipulation of the argument exec results in code injection. The attack may be performed from remote. The exploit has been made public and could be used. The reported GitHub issue was closed automatically due to inactivity.	2026-08-19	7.3	CVE-2026-76760
chenhg5--cc-connect	A vulnerability was identified in chenhg5 cc-connect up to 1.4.1. This affects the function shellExecCommand of the file core/engine.go of the component Management API. Such manipulation of the argument exec leads to os command injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The reported GitHub issue was closed automatically due to inactivity.	2026-08-19	7.3	CVE-2026-76761
chirpmyradio--CHIRP	chirpmyradio CHIRP before 39178db allows eval injection via crafted CSV data. This occurs in _clean_tmode in drivers/kenwood_itm.py.	2026-08-23	7.8	CVE-2026-78136

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco BroadWorks	A vulnerability in the Open Client Interface (OCI) XML Parser of Cisco BroadWorks could allow an unauthenticated, remote attacker to read sensitive configuration information on an affected system. This vulnerability exists because XML entries are improperly parsed due to external entity resolution being allowed by default. An attacker could exploit this vulnerability by sending a crafted XML message to the Open Client Interface & Provisioning (OCI-P) service. A successful exploit could allow the attacker to view sensitive files from the filesystem with the privileges of the Cisco BroadWorks user.	2026-08-19	7.5	CVE-2026-20320
Cisco--Cisco Crosswork Planning	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Crosswork engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20030 are related to improper neutralization of special elements used in a SQL command issues that are grouped under the Common Weakness Enumeration (CWE) CWE-89.	2026-08-19	10	CVE-2026-20030
Cisco--Cisco Crosswork Planning	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Crosswork engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20357 are related to missing authentication for critical function issues that are grouped under the Common Weakness Enumeration (CWE) CWE-306.	2026-08-19	10	CVE-2026-20357
Cisco--Cisco Crosswork Planning	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Crosswork engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20358 are related to external control of the file system issues that are grouped Common Weakness Enumeration (CWE) CWE-73.	2026-08-19	10	CVE-2026-20358
Cisco--Cisco Crosswork Planning	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Crosswork engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20359 are related to insufficiently protected credentials issues that are grouped under the Common Weakness Enumeration (CWE) CWE-522.	2026-08-19	9.9	CVE-2026-20359
Cisco--Cisco Secure Workload	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Secure Workload engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20315 are related to improper access control issues that are grouped under the Common Weakness Enumeration (CWE) CWE-284.	2026-08-19	10	CVE-2026-20315
Cisco--Cisco Secure Workload	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Secure Workload engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20317 are related to improper authentication issues that are grouped under the Common Weakness Enumeration (CWE) CWE-287.	2026-08-19	10	CVE-2026-20317
Cisco--Cisco Secure Workload	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Secure Workload engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20231 are related to improper neutralization of special elements issues that are grouped under the Common Weakness Enumeration (CWE) CWE-74.	2026-08-19	9.9	CVE-2026-20231
Cisco--Cisco Secure Workload	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Secure Workload engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20318 are related to improper input validation issues that are grouped under the Common Weakness Enumeration (CWE) CWE-20.	2026-08-19	9.6	CVE-2026-20318
Cisco--Cisco Secure Workload	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Secure Workload engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities. The vulnerabilities tracked by CVE-2026-20319 are related to buffer management issues that are grouped under the Common Weakness Enumeration (CWE) CWE-119.	2026-08-19	7.5	CVE-2026-20319

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
CleanTalk Inc-- Security & Malware scan by CleanTalk	Unauthenticated SQL Injection in Security & Malware scan by CleanTalk <= 2.184 versions.	2026-08-20	9.3	CVE-2026-66593
Cloud Foundry Foundation--BOSH CLI	Command Injection in BOSH CLI tool on windows in Cloud Foundry allows a remote attacker to execute arbitrary shell commands via command injection vulnerabilities	2026-08-21	7.5	CVE-2026-47827
cloudnative-pg-- cloudnative-pg	CloudNativePG is a platform designed to manage PostgreSQL databases within Kubernetes environments. Prior to 1.28.4 and 1.29.2, CloudNativePG embedded cleartext role passwords in `ALTER ROLE` and `CREATE ROLE` statements generated by SetUserPassword in pkg/management/postgres/utills/roles.go and appendPasswordOption in internal/management/controller/roles/postgres.go. When pg_stat_statements was preloaded with track_utility enabled and an untrusted tenant held pg_monitor or pg_read_all_stats, the tenant could recover platform-managed superuser or application-owner passwords, reconnect through enabled superuser TCP access, and execute operating system commands in the database pod with `COPY ... FROM PROGRAM`. Clusters using SCRAM-SHA-256 verifiers in managed-role Secrets were not affected. This issue is fixed in versions 1.28.4, 1.29.2, and 1.30.0.	2026-08-20	8.5	CVE-2026-55765
Cloudways--Breeze	Unauthenticated Arbitrary Content Deletion in Breeze <= 2.5.12 versions.	2026-08-18	8.2	CVE-2026-73356
cmsMinds--Pay with Contact Form 7	Unauthenticated Sensitive Data Exposure in Pay with Contact Form 7 <= 1.0.4 versions.	2026-08-19	7.5	CVE-2026-73384
code-projects-- Assessment Management	A vulnerability was detected in code-projects Assessment Management 1.0. The affected element is an unknown function of the file /welcome.php. The manipulation of the argument userid results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	2026-08-19	7.3	CVE-2026-76762
code-projects-- Barangay Resident Profiling Management System	A vulnerability was determined in code-projects Barangay Resident Profiling Management System 1.0. Affected is an unknown function of the file residents.php of the component Resident Search Functionality. This manipulation of the argument Search causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	2026-08-23	7.3	CVE-2026-78143
code-projects-- Employee Management System	A flaw has been found in code-projects Employee Management System 1.0. The impacted element is an unknown function of the file /process/aprocess.php of the component Admin Login Endpoint. This manipulation of the argument mailuid causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2026-08-20	7.3	CVE-2026-76764
code-projects-- Hospital Information System	A flaw has been found in code-projects Hospital Information System 1.0. The impacted element is the function User::login of the file includes/users/UsersController.php of the component User Login Handler. This manipulation of the argument email causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	2026-08-19	7.3	CVE-2026-76574
code-projects-- Online Job Portal System	A vulnerability has been found in code-projects Online Job Portal System 1.0. The impacted element is an unknown function of the file /ForPass.php of the component Password Recovery. Such manipulation of the argument txtUserName leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-08-19	7.3	CVE-2026-75986
code-projects-- Simple Inventory System	A vulnerability has been found in code-projects Simple Inventory System 1.0. Affected by this issue is some unknown functionality of the file /delete.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-08-20	7.3	CVE-2026-76990
code-projects-- Task Management System	A vulnerability was identified in code-projects Task Management System 1.0. This affects the function Operation::select_with_multiple_condition of the file /index.php of the component Login Form. Such manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2026-08-18	7.3	CVE-2026-75778
CodeAstro-- Apartment Visitor Management System	A vulnerability was determined in CodeAstro Apartment Visitor Management System 1.0. Affected is an unknown function of the file /apartment-visitor/forgotpw.php. Executing a manipulation of the argument secode can lead to sql injection. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-20	7.3	CVE-2026-77019
CodeAstro-- Apartment Visitor	A vulnerability was identified in CodeAstro Apartment Visitor Management System 1.0. Affected by this vulnerability is an unknown functionality of the file password-recovery.php. The manipulation of the argument email leads to sql injection.	2026-08-20	7.3	CVE-2026-77020

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	Remote exploitation of the attack is possible. The exploit is publicly available and might be used.			
Codexpert, Inc--ThumbPress	Unauthenticated Broken Access Control in ThumbPress < 6.5 versions.	2026-08-18	7.5	CVE-2026-32549
CodexThemes--TheGem (Elementor)	Unauthenticated SQL Injection in TheGem (Elementor) <= 5.12.3 versions.	2026-08-20	9.3	CVE-2026-66609
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, there is a Reflected Cross-Site Scripting (XSS) vulnerability in the testing OQL query functionality. This issue has been fixed in version 3.2.3.	2026-08-21	8	CVE-2026-30826
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, there is a Reflected Cross-Site Scripting (XSS) vulnerability in the synchro import script. This issue has been fixed in version 3.2.3.	2026-08-21	8	CVE-2026-30890
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, 3.2.3, there is a Reflected Cross-Site Scripting (XSS) vulnerability in pages/tagadmin.php. This issue has been fixed in version 3.2.3.	2026-08-21	8	CVE-2026-31803
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, there is a Reflected Cross-Site Scripting (XSS) vulnerability in the universal search. This issue has been fixed in version 3.2.3.	2026-08-21	8	CVE-2026-31880
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, users can access to unauthorized object information through the search operation. This issue has been fixed in version 3.2.3.	2026-08-21	8.8	CVE-2026-31936
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, there was a Reflected Cross-Site Scripting (XSS) vulnerability in the foreign key search criteria API. This issue has been fixed in version 3.2.3.	2026-08-21	8.8	CVE-2026-33240
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, authentication bypass allows unauthenticated remote attackers to execute arbitrary PHP files from the env-production directory on a new iTop instance in the production environment. This issue has been fixed in version 3.2.3.	2026-08-21	8.6	CVE-2026-34741
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, iTop returns different responses for valid/invalid usernames depending on multiple factors in the reset password mechanism, leading to user enumeration. This issue has been fixed in version 3.2.3.	2026-08-21	7.5	CVE-2026-27462
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, inline images that are accessible without being authenticated are protected by a weak 24-bit pseudo-random secret. This issue has been fixed in version 3.2.3.	2026-08-21	7.5	CVE-2026-27490
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, iTop has a reflected Cross-Site Scripting (XSS) vulnerability in its dashboard revert functionality with the parameter dashboard_id in /pages/ajax.render.php. This issue has been fixed in version 3.2.3.	2026-08-21	7.3	CVE-2026-30819
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, there is a Reflected Cross-Site Scripting (XSS) vulnerability in the dashboard save functionality. This issue has been fixed in version 3.2.3.	2026-08-21	7.1	CVE-2026-30865
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, unauthenticated users can access uploaded sensitive via sniffed url. This issue has been fixed in version 3.2.3.	2026-08-21	7.5	CVE-2026-30866
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, only classes present in the SELECT clause are protected by the silos access check in OQL. This issue has been fixed in version 3.2.3.	2026-08-21	7.7	CVE-2026-34948
COMFAST--CF-N1-S	A flaw has been found in COMFAST CF-N1-S 2.6.0.1. This impacts the function sub_44B438 of the file /cgi-bin/mbox-config?method=SET&section=ptest_ssid of the component CGI Interface. This manipulation of the argument ssid causes os command injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2026-08-18	9.1	CVE-2026-75094
Comfast--CF-N1-S	A flaw has been found in Comfast CF-N1-S 2.6.0.1. This affects the function get_para_from_uri of the file /cgi-bin/mbox-config of the component URI Parameter Parsing. This manipulation of the argument width/height causes stack-based buffer overflow. The attack can be initiated remotely.	2026-08-19	10	CVE-2026-76008
Comfast--CF-N1-S	A security flaw has been discovered in Comfast CF-N1-S 2.6.0.1. Affected by this issue is the function sub_44B438 of the file /cgi-bin/mbox-config?method=SET&section=ptest_ssid of the component SSID Configuration. The manipulation of the argument ssid results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	2026-08-20	9.9	CVE-2026-77022

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Comfast--CF-N1-S	A vulnerability was found in Comfast CF-N1-S 2.6.0.1. This impacts the function sub_44B50C of the file /cgi-bin/mbox-config?method=SET&section=pctest_channel of the component Web Management. The manipulation results in stack-based buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.	2026-08-20	9.9	CVE-2026-77148
Comfast--CF-N1-S	A security flaw has been discovered in Comfast CF-N1-S 2.6.0.1. Affected by this issue is the function system of the file /cgi-bin/mbox-config?method=SET&section=ntp_timezone. The manipulation of the argument timestr results in command injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-08-21	9.9	CVE-2026-77683
Comfast--CF-N1-S	A vulnerability was found in Comfast CF-N1-S 2.6.0.1. The affected element is the function sub_41AD7C of the file /cgi-bin/mbox-config?method=SET&section=ntp_timezone of the component Web Management. The manipulation of the argument timestr/ntp_client_enabled results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2026-08-22	9.9	CVE-2026-78050
Comfast--CF-N1-S	A flaw has been found in Comfast CF-N1-S 2.6.0.1. This impacts the function sprintf of the file /cgi-bin/mbox-config?method=SET&section=pctest_sn. Executing a manipulation of the argument sn can lead to command injection. The attack can be launched remotely. The exploit has been published and may be used.	2026-08-20	7.4	CVE-2026-77004
coturn--coturn	Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.13.0, an authenticated TURN user can place printf-style format specifiers in the STUN USERNAME or REALM attribute, which passes is_secure_string() validation and is embedded into Redis keys at nine call sites in src/apps/relay/ns_ioalib_engine_impl.c. send_message_to_redis() in src/apps/relay/hiredis_libevent2.c then passes the attacker-controlled key as the format argument to redisAsyncCommand() while supplying only one variadic value, causing hiredis redisvFormatCommand() to read past the va_list. Exploitation can crash the coturn process and terminate active TURN sessions or disclose stack memory into Redis. This issue is fixed in version 4.13.0.	2026-08-19	7.1	CVE-2026-68553
COVESA--Open1722	COVESA Open1722 through 0.9.2 contains a stack buffer overflow vulnerability that allows unauthenticated remote attackers to write past the end of a fixed 15-slot stack array by sending a crafted UDP datagram containing more than 15 ACF-CAN messages. The avtp_to_can() function increments its write index without bounding it against the caller-supplied array size, and because the listener accepts datagrams from any sender matching a hardcoded unauthenticated stream ID transmitted in plaintext, attackers can corrupt adjacent stack memory to achieve arbitrary code execution or denial of service.	2026-08-17	7.5	CVE-2026-73522
COVESA--Open1722	COVESA Open1722 through 0.9.2 contains an integer truncation vulnerability in acf-can-listener.c that allows unauthenticated remote attackers to cause the CAN listener to transmit process stack memory onto the CAN bus by sending a rejected UDP datagram with a matching AVTP stream ID. The num_can_msgs variable declared as uint8_t truncates the -1 error return value from avtp_to_can() to 255, causing a write loop to iterate 255 times over a 15-slot stack array and leak approximately 18 KB of adjacent stack memory as roughly 240 CAN frames to any recipient on the CAN bus.	2026-08-17	7.5	CVE-2026-73523
Cozmoslabs--TranslatePress	Unauthenticated Cross Site Scripting (XSS) in TranslatePress <= 3.3.2 versions.	2026-08-20	7.1	CVE-2026-66582
cozmoslabs--TranslatePress Translate Multilingual sites with AI Translation	The TranslatePress - Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to unauthenticated Stored Cross-Site Scripting in versions up to and including 3.2.5. The special gettext markers '#!trpst#' and '#!trpen#' are unconditionally rewritten to '<' and '>' by translate_page() in includes/class-translation-render.php (lines 538-539). Because those markers are plain text with no HTML-special characters, an unauthenticated attacker can embed them in a comment; the markers survive wp_kses, and when the post is viewed in a secondary language the substitution turns the attacker's '#!trpst#img ... #!trpen#' into a real tag. remove_tags_from_output() only strips <script>/<style>, so an executes in the visitor's browser.	2026-08-19	7.2	CVE-2026-75981
crawlab-team--crawlab	Crawlab fails to verify user ownership or administrative role on the password-change endpoint, allowing any authenticated user to reset any account's password. Attackers can enumerate user accounts through the user listing endpoint and change administrator credentials to achieve full account takeover and arbitrary code execution.	2026-08-17	8.8	CVE-2026-75103

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Crocoblock. Jetimpex Inc.-- JetAppointment	Unauthenticated SQL Injection in JetAppointment <= 2.5.2 versions.	2026-08-18	9.3	CVE-2026-73365
Crocoblock. Jetimpex Inc.-- JetEngine	Unauthenticated Remote Code Execution (RCE) in JetEngine <= 3.8.14 versions.	2026-08-19	9.8	CVE-2026-66613
Crocoblock. Jetimpex Inc.-- JetEngine	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.14.1 versions.	2026-08-20	7.1	CVE-2026-66581
Cwicly--Cwicly	Contributor Remote Code Execution (RCE) in Cwicly <= 1.4.4 versions.	2026-08-18	9.9	CVE-2026-32444
David Lingren-- Media Library Assistant	Author Arbitrary File Upload in Media Library Assistant <= 3.39 versions.	2026-08-20	9.1	CVE-2026-66600
decolua--9router	9Router is an AI router & token saver. In 0.5.4 and earlier, the POST /api/auth/oidc/test endpoint in src/app/api/auth/oidc/test/route.js passes the user-controlled issuerUrl parameter to fetchOidcDiscovery() in src/lib/auth/oidc.js without restricting private or loopback destinations, allowing unauthenticated attackers when dashboard login is disabled to scan internal services and reflect OIDC discovery fields including token_endpoint and jwks_uri.	2026-08-17	8.6	CVE-2026-56677
decolua--9router	The POST /api/provider-nodes/validate route in 9router takes a caller-supplied baseUrl and issues server-side HTTP requests to it, guarding the destination with assertPublicUrl from src/shared/utls/ssrfGuard.js. That guard compares hostname strings only: it resolves no DNS, does not revalidate after a redirect, and its IPv4-mapped IPv6 branch is unreachable. The branch matches ^::ffff:(\d+\.\d+\.\d+\.\d+)\$, but the WHATWG URL parser canonicalizes such literals to hextets before the guard runs, so new URL("http://[::ffff:127.0.0.1]/").hostname yields [::ffff:7f00:1] and the pattern is tested against a string it is never handed. Every IPv4-mapped address therefore passes, and http://[::ffff:7f00:1] and http://[::ffff:a9fe:a9fe] reach loopback and link-local metadata addresses; a hostname whose A record points at an internal address passes as well because no resolution occurs. In the custom-embedding branch the upstream response body is truncated to 200 bytes and returned to the caller whenever the upstream status is neither 2xx nor 401 nor 403, which discloses the beginning of internal responses, and the other validation types remain usable for blind internal port scanning through status and timing differences. The caller-supplied apiKey is forwarded to the internal destination as an Authorization Bearer header. A dashboard session is required by default, and none is required when requireLogin is disabled.	2026-08-20	8.5	CVE-2026-72860
DeDeCMS-- DeDeCMS	A security vulnerability has been detected in DeDeCMS 53_1_UTF8. This vulnerability affects unknown code of the file /plus/advancedsearch.php. Such manipulation of the argument sql leads to sql injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2026-08-20	7.3	CVE-2026-76783
DeKnows--PDF Smart Viewer for Elementor	Unauthenticated Server Side Request Forgery (SSRF) in PDF Smart Viewer for Elementor <= 1.0.4 versions.	2026-08-18	7.2	CVE-2026-32473
Dell--Alienware Command Center (AWCC)	Dell Alienware Command Center (AWCC), versions prior to 6.14.20.0, contain a Least Privilege Violation vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-08-18	7.3	CVE-2026-59915
Dell--AppSync	Dell AppSync Version 4.6.0.0, Dell Metro Node Version 8.0.0, Dell UCC Edge Version 3.0.1, Dell VxRail Version 8.0.322, Dell PowerMax Version 10.3.0, Dell Unity Version 5.4, Dell PowerFlex Manager Version 4.5.4, Dell PowerFlex Intelligent Catalog Versions 46.377.00 and 46.382.00 and Dell PowerFlex Rack version 4.5.4 and prior versions, contain(s) an UNIX Symbolic Link (Symlink) Following vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-08-18	7.3	CVE-2026-32657
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain a Missing Authorization vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-08-19	8.8	CVE-2026-58565
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain a Deserialization of Untrusted Data vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-08-19	7.8	CVE-2026-49816
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain a Deserialization of Untrusted Data vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-08-19	7.8	CVE-2026-49817

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-08-19	7.8	CVE-2026-53477
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-08-19	7.3	CVE-2026-56797
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain a Missing Authorization vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-08-19	7.3	CVE-2026-58562
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain an Incorrect Default Permissions vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	2026-08-19	7.8	CVE-2026-58564
Dell--ObjectScale	Dell ObjectScale, versions prior to 4.3.0.1, contain(s) an Uncontrolled Search Path Element vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-08-17	7.3	CVE-2026-56090
Dell--ObjectScale	Dell ObjectScale, versions prior to 4.3.0.1, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2026-08-17	7.3	CVE-2026-56685
Dell--ObjectScale	Dell ObjectScale, versions prior to 4.3.0.1, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-08-17	7.8	CVE-2026-56686
Dell--ObjectScale	Dell ObjectScale, versions prior to 4.3.0.1, contain(s) a Path Traversal vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	2026-08-17	7.1	CVE-2026-59909
Dell--ObjectScale	Dell ObjectScale, versions prior to 4.3.0.1, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-08-17	7.8	CVE-2026-59910
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	2026-08-19	8.8	CVE-2026-54795
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Script injection.	2026-08-19	8.1	CVE-2026-70422
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-08-19	8.8	CVE-2026-71176
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains a Server-Side Request Forgery (SSRF) vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-08-19	7.2	CVE-2026-54794
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	2026-08-19	7.2	CVE-2026-54796
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Script injection.	2026-08-19	7.1	CVE-2026-56088
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Privilege Management vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-08-19	7.2	CVE-2026-70421
Dell--PowerStore 500T	Dell PowerStore SDNAS, contains an Out-of-bounds Write vulnerability in the SMB/CIFS. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Denial of service and Remote execution. This is a Critical vulnerability as a remote user could send a specially crafted SMB packet and cause a crash, that is persistent in case automatic restarts are enabled. Additionally, a more sophisticated attacker could use the same vulnerability for Remote Code execution.	2026-08-18	9.8	CVE-2026-67271

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--PowerStore 500T	Dell PowerStore contains a Missing Authorization vulnerability. An attacker with access to a mapped host could exploit this vulnerability to read from or write to LUNs that the host is not authorized to access, bypassing per-initiator LUN access controls and leading to protection mechanism bypass.	2026-08-18	8.1	CVE-2026-67262
Dell--PowerStore 500T	Dell PowerStore SDNAS contains a Buffer Copy without Checking Size of Input vulnerability in the NFS/RPC. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Command execution and Denial of service.	2026-08-18	8.1	CVE-2026-70415
Dell--RecoverPoint for Virtual Machines	Dell RecoverPoint for VMs, versions 6.0.3 and 6.0.3.1, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	2026-08-19	7.2	CVE-2026-23501
Dell--Watchdog Timer Driver	Dell Watchdog Timer Driver versions prior to 2.0.0.1 contain an Exposed IOCTL with Insufficient Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Privilege Escalation.	2026-08-18	8.8	CVE-2026-61407
Derek Herman--OptionTree	Editor PHP Object Injection in OptionTree <= 2.7.3 versions.	2026-08-18	7.2	CVE-2026-66620
deskflow--deskflow	Deskflow is a keyboard and mouse sharing app. From 1.17.0 until continuous build 1.26.0.296, a malicious Deskflow server can send an odd-length DSOP vector to ServerProxy::setOptions() in src/lib/client/ServerProxy.cpp, causing the missing value after the final option key to be read beyond the vector during the PacketStreamFilter::filterEvent to ServerProxy::handleData() to ServerProxy::parseHandshakeMessage() call chain and crash the connected client. This issue is fixed in continuous build 1.26.0.296.	2026-08-17	8.2	CVE-2026-63409
deskflow--deskflow	Deskflow is a keyboard and mouse sharing app. Prior to continuous build 1.26.0.299, a remote unauthenticated Deskflow server can send kMsgDSetOptions (DSOP) values to ServerProxy::setOptions() in src/lib/client/ServerProxy.cpp so that the value following a modifier option poisons m_modifierTranslationTable, after which ServerProxy::translateKey() or ServerProxy::translateModifierMask() indexes the seven-row s_translationTable or s_masks arrays out of bounds, disclosing four bytes at an attacker-selected relative offset or crashing the connected client; an odd option count also causes an out-of-bounds OptionsList read. This issue is fixed in continuous build 1.26.0.299.	2026-08-17	8.2	CVE-2026-65832
determined-ai--determined	Determined fails to authorize requests on the generic task kill, pause, and unpause endpoints in the API handlers. Authenticated attackers can disrupt other users' workloads by terminating, pausing, or unpausing tasks they do not own.	2026-08-17	7.1	CVE-2026-75109
DevItems--HashBar WordPress Notification Bar	Cross-Site Request Forgery (CSRF) vulnerability in DevItems HashBar - WordPress Notification Bar allows Cross Site Request Forgery. This issue affects HashBar - WordPress Notification Bar: from n/a through 2.0.0.	2026-08-18	8.8	CVE-2026-66602
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, an unauthenticated attacker could send a single request with a crafted color_scheme_id (or dark_scheme_id) cookie to inject arbitrary HTML into a Discourse page. Because the cookie value was rendered into a color scheme tag without escaping, the attacker could break out of the attribute and inject a tag that bypassed Discourse's nonce-based Content Security Policy, resulting in arbitrary JavaScript execution in visitors' browsers. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-17	9.3	CVE-2026-55674
django-cms--django-cms	django CMS is an easy-to-use and developer-friendly enterprise content management system powered by Django. Prior to 5.0.8, the move_plugin endpoint in cms/admin/placeholderadmin.py accepts an attacker-controlled plugin_parent value without rejecting a plugin's own identifier or a descendant identifier. A staff user with plugin-change permission under CMS_PERMISSION can create a parent_id cycle in the plugin tree. The _get_descendants_cte and _get_ancestors_cte queries in cms/models/pluginmodel.py have no cycle guard, so get_descendants() and later rendering, copy, or delete operations can recurse indefinitely or reach a database recursion limit, corrupting the tree and consuming request workers. This issue is fixed in versions 5.0.8.	2026-08-20	7.1	CVE-2026-54623
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.6, Dokploy's organization.inviteMember tRPC procedure in apps/dokploy/server/api/routers/organization.ts allows a user with member:create permission to invite an account with the owner role, while packages/server/src/services/user.ts allows a privileged self-hosted user to create an account with an arbitrary role, enabling permanent organization takeover because owner roles cannot be demoted. This issue is fixed in version 0.29.6.	2026-08-17	8	CVE-2026-45790

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dolusoft Software Technologies--Fortilogger	Missing Authorization vulnerability in Dolusoft Software Technologies Fortilogger allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Fortilogger: before 6.1.5.9.	2026-08-17	7.5	CVE-2026-16467
Dolusoft Software Technologies--Sonlogger	Missing Authorization vulnerability in Dolusoft Software Technologies Sonlogger allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Sonlogger: from v6.6.6 before 6.7.4.8.	2026-08-17	7.5	CVE-2026-16471
droundy--append-only-vec	The append-only-vec crate 0.1.9 for Rust can trigger execution of malicious code when compiling a project that uses the crate, because it has a rogue dependency that registers with a command-and-control server to offer arbitrary code execution.	2026-08-21	9.8	CVE-2026-77650
droundy--arrayref	The arrayref crate 0.3.10 for Rust can trigger execution of malicious code when compiling a project that uses the crate, because it has a rogue dependency that registers with a command-and-control server to offer arbitrary code execution.	2026-08-21	9.8	CVE-2026-77651
droundy--internment	The internment crate 0.8.7 for Rust can trigger execution of malicious code when compiling a project that uses the crate, because it has a rogue dependency that registers with a command-and-control server to offer arbitrary code execution.	2026-08-21	9.8	CVE-2026-77649
e-plugins--Directory Pro	Unauthenticated SQL Injection in Directory Pro <= 2.5.8 versions.	2026-08-20	9.3	CVE-2026-66649
Edge Themes--Shuffle	Unauthenticated Local File Inclusion in Shuffle <= 1.8 versions.	2026-08-20	8.1	CVE-2025-15637
EDGE22 Studios Ltd.--GP Premium	Contributor Arbitrary File Upload in GP Premium <= 2.5.5 versions.	2026-08-18	9.9	CVE-2026-66627
EFM--ipTIME A3004T	A vulnerability was detected in EFM ipTIME A3004T 14.19.0. The affected element is the function httpcon_check_session_url of the component Session Validation. Performing a manipulation results in improper authentication. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-17	10	CVE-2026-19977
electerm--electerm	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. Prior to 3.11.11, electerm constructs operating system commands in src/app/lib/fs.js by interpolating untrusted file paths into the rmrf(), mv(), and cp() functions. A malicious SSH or SFTP server can provide a filename containing quote characters and shell metacharacters, and a victim can cause that filename to reach the affected operation during remote-to-local transfer, conflict renaming, copying, moving, or removal. The generated `rm -rf`, mv, `cp -r`, PowerShell Remove-Item, Move-Item, or Copy-Item command can then interpret the filename as shell syntax. This allows arbitrary command execution with the electerm desktop user's privileges on POSIX and Windows systems, enabling data exfiltration, file modification, malware installation, or denial of service. This issue is fixed in version 3.11.11.	2026-08-19	8.8	CVE-2026-49255
electerm--electerm	electerm is an open-sourced terminal/ssh/sftp/telnet/serialport/RDP/VNC/Spice/ftp client. Prior to 3.11.11, electerm uses remote-supplied filenames directly with path.join() while receiving Zmodem and Trzsz transfers. In src/app/server/zmodem.js, prepareReceiveFile() joins the filename to the user-selected save path, and in src/app/server/trzsz.js, getUniqueFilePath(), the openSaveFile() callback, and the savedFilePaths mapping construct destinations without sanitization. A malicious SSH server or remote shell can provide a filename containing traversal components such as ../escaped.txt or ../../.bashrc. When the victim accepts the transfer and selects a download directory, electerm can write outside that directory and overwrite files accessible to the desktop user, potentially changing sensitive configuration or impairing availability. This issue is fixed in version 3.11.11.	2026-08-19	7.1	CVE-2026-49253
Elementor--Elementor Pro	Unrestricted Upload of File with Dangerous Type vulnerability in Elementor Elementor Pro allows Using Malicious Files. This issue affects Elementor Pro: from n/a through 4.2.1.	2026-08-19	9	CVE-2026-32475
EmilStenstrom--justhtml	justhtml before 1.15.0 contains multiple security issues in URL sanitization helpers (clean_url_value/clean_url_in_js_string), HTML serialization, Markdown passthrough (html_passthrough=True), and several custom sanitization-policy edge cases. Depending on configuration, an attacker can bypass sanitization to inject active HTML and JavaScript - for example via encoded javascript: URLs, backslash-based relative URLs resolved as remote hosts, markup-breaking programmatic element/attribute names or HTML comments, raw </textarea> reintroduction through Markdown passthrough, or preserved <style>/<meta http-equiv=refresh>/<base href> tags in custom policies. Most custom-policy issues do	2026-08-23	9.8	CVE-2026-5388

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	not affect the default sanitize=True configuration; they primarily affect helper APIs, programmatic DOM construction, html_passthrough=True, and custom policies/transform pipelines.			
EmilStenstrom--justhtml	justhtml before 1.16.0 contains multiple HTML sanitization bypass issues that can allow active/dangerous content (e.g., script or style) to survive sanitization, potentially leading to cross-site scripting. The issues primarily affect advanced usage rather than the default JustHTML(..., sanitize=True) path for ordinary parsed HTML: mutating or reusing sanitization policy objects (including exported defaults) could weaken later sanitization; programmatic DOM input to sanitize()/sanitize_dom() could miss mixed-case tag names (e.g., ScRiPt, StYlE); crafted programmatic doctype names could serialize into active markup; and custom policies preserving SVG or MathML could allow animation elements, presentation attributes with external url(...) references, or DOM trees mislabeled as namespace="html" to bypass foreign-content checks. Fixed in 1.16.0.	2026-08-23	9.8	CVE-2026-7808
EmilStenstrom--justhtml	justhtml versions <= 1.11.0 (fixed in 1.12.0) do not sufficiently escape HTML-significant characters (angle brackets) in text nodes when converting a parsed document to Markdown via to_markdown(). While a small set of Markdown metacharacters are escaped, characters such as < and > are preserved, so untrusted input that is safe in to_html() - including entity-decoded text (e.g. <script>) or text from RCDATA/RAWTEXT-parsed elements like <title>, <textarea>, <noscript>, and <plaintext> - can be emitted as raw HTML in the Markdown output, enabling a sanitizer bypass and potential cross-site scripting when that output is rendered.	2026-08-23	9.8	CVE-2026-8445
EmilStenstrom--justhtml	justhtml before 1.18.0 contains multiple low-severity denial-of-service issues in CSS selector handling and linkification. Applications that evaluate attacker-controlled selector strings (via query(), matches(), or selector-based transforms), run selector matching over very large untrusted documents, construct DOM trees from untrusted structure, or enable linkification over attacker-controlled text may consume disproportionate CPU or memory. Triggers include oversized selectors, large selector lists, oversized compound selectors, long combinator chains, deeply nested functional pseudo-classes, repeated token/positional matching, cyclic DOM graphs causing non-terminating traversal, and punctuation-heavy or trailing-bracket linkification input. These are availability-only concerns and do not by themselves allow script execution, data disclosure, or sanitizer bypass. Default JustHTML(sanitize=True) usage is not expected to be exposed, since selectors are normally supplied by application code.	2026-08-23	7.5	CVE-2026-4671
EmilStenstrom--justhtml	justhtml through 1.9.1 (fixed in 1.10.0) is vulnerable to uncontrolled recursion leading to denial of service. During JustHTML() construction, TreeBuilder.finish() unconditionally calls _populate_selectedcontent(), which recursively traverses the DOM tree via _find_elements()/_find_element() without a depth bound. An attacker who can supply HTML for parsing can provide deeply nested elements (e.g., ~1000 nested <div> tags, roughly 11 KB) to exceed CPython's default recursion limit and trigger an unhandled RecursionError, which may abort parsing, fail requests, or terminate a worker/process depending on the host application's exception handling.	2026-08-23	7.5	CVE-2026-9769
Eric Teubert--Podlove Podcast Publisher	Unauthenticated Cross Site Scripting (XSS) in Podlove Podcast Publisher <= 4.5.4 versions.	2026-08-20	7.1	CVE-2026-66615
ether--etherpad	Etherpad is a real-time collaborative editor. Prior to 3.3.1, result.appendSpan in src/static/js/domline.ts interpolates the start attribute of a numbered list directly into an unquoted ol start attribute before assigning the generated markup to node.innerHTML. ImportEtherpad.setPadRaw in src/node/utils/ImportEtherpad.ts accepts attacker-controlled attribute-pool values from a crafted .etherpad import, including list:number1 and a malicious start value. Any user with write access to a pad can store markup that executes as cross-site scripting when another user opens the pad or /timeslider, including when an administrator views the pad. This issue is fixed in version 3.3.1.	2026-08-19	9.6	CVE-2026-55085
ether--etherpad	Etherpad is a real-time collaborative editor. From 2.1.0 until 3.1.0, Etherpad's src/node/handler/APIHandler.ts authorizes requests to /api/2/* in the authorization_code OAuth path by using requiredClaims with the admin claim. This check requires only that the claim exists, while src/node/security/OAuth2Provider.ts issues admin: false for configured non-admin users. A non-admin user with a valid signed token can therefore invoke administrative functions including setHTML, setText, appendText, deletePad,	2026-08-19	9.9	CVE-2026-55089

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	copyPad, movePad, restoreRevision, anonymizeAuthor, listAllPads, and listAuthorsOfPad, allowing disclosure, modification, or deletion of pads across the instance. This issue is fixed in version 3.1.0.			
etrue--WPematico RSS Feed Fetcher	The WPematico RSS Feed Fetcher plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a missing capability check on the wpematico_import_settings function in all versions up to, and including, 2.8.24. This makes it possible for authenticated attackers, with subscriber-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access.	2026-08-22	8.8	CVE-2026-19883
evershopcommerce--evershop	The customer update route in EverShop is declared with "access": "public" in packages/evershop/src/modules/customer/api/updateCustomer/route.json, which causes the admin authentication middleware to call next() without checking the caller, and no customer-session middleware guards the route; the only middleware in the chain parses the JSON body. The handler in updateCustomer.js then loads the customer by the uuid taken from the URL path and writes the supplied fields back to that record, hashing a password if one is provided, without verifying that the caller owns the record. An unauthenticated request carrying a known customer uuid can therefore overwrite that customer's email address and password and read back the updated record from the 200 response, taking over the account and locking out its owner. Customer uuids are exposed through order confirmation email links and administrative URLs. Version 2.2.1 changes the route to "access": "private".	2026-08-20	9.8	CVE-2026-72843
evidentlyai--evidently	Evidently UI fails to properly validate the filename parameter in the dataset materialization endpoint, allowing unauthenticated attackers to read arbitrary files outside the workspace directory. Attackers can supply traversal sequences or absolute paths in the filename field to access system files, which are then materialized into datasets and retrieved through the download endpoint.	2026-08-17	7.5	CVE-2026-75111
ezoic--Ezoic	Unauthenticated Broken Authentication in Ezoic <= 2.22.11 versions.	2026-08-18	7.5	CVE-2026-32481
facebookresearch--hydra	Hydra is a framework for elegantly configuring complex applications. Prior to 1.3.4, hydra.utils.instantiate() resolves and calls Python objects selected by configuration through _resolve_target() in hydra/_internal/instantiate/_instantiate2.py, allowing attacker-controlled target values and arguments to choose dangerous callables. A consuming application, library, CLI workflow, or model loader that passes untrusted configuration, CLI overrides, or model metadata into hydra.utils.instantiate() can therefore execute arbitrary code in its own process, including reading or modifying files and credentials or terminating the process. Version 1.3.4 adds target blocking with an explicit HYDRA_INSTANTIATE_ALLOWLIST_OVERRIDE escape hatch. This issue is fixed in version 1.3.4.	2026-08-21	7.8	CVE-2026-68508
Fahad Mahmood--WP Sort Order	Unauthenticated Broken Access Control in WP Sort Order <= 1.3.5 versions.	2026-08-18	7.5	CVE-2026-28567
Faydam Innovation Inc.--FAYDAM Datalogger	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Faydam Innovation Inc. FAYDAM Datalogger allows SQL Injection. This issue affects FAYDAM Datalogger: from 2.7.1 before 2.8.0.	2026-08-19	9.8	CVE-2026-16019
fbeta-GmbH--ePA3-Service-OpenSource	ePA 3.x Integration implements the authorization workflow and writes Medical Information Objects to Germany's electronic patient record. Prior to 1.3.0, ePA 3.x Integration performs VAU server certificate validation in app/vau/VAUProtokoll.py without anchoring the signed_vau_server_pub_keys and AUT_VAU_CertData certificate path to independent trusted material. A network-positioned attacker between the DiGA backend and the ePA system can intercept the VAU handshake, supply attacker-controlled certificate and key material, and satisfy the circular trust relationship. Because TLS certificate verification is also disabled in affected versions, no independent server-authentication layer prevents the attack. The attacker can impersonate the VAU server, control the negotiated session keys, and read or modify all encrypted VAU traffic. This issue is fixed in version 1.3.0.	2026-08-18	9.1	CVE-2026-52723
fbeta-GmbH--ePA3-Service-OpenSource	ePA 3.x Integration implements the authorization workflow and writes Medical Information Objects to Germany's electronic patient record. Prior to 1.3.0, ePA 3.x Integration leaves request_counter unchanged in app/vau/VAUProtokoll.py while constructing VAU messages. The frozen client request counter causes the server side to reuse AES-GCM nonce and key combinations across responses. A network attacker who collects repeated ciphertexts can recover the XOR of plaintexts and use predictable inner HTTP headers and JSON fields to recover sensitive data,	2026-08-18	7.4	CVE-2026-50577

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	including patient health records. Repeated nonces can also enable recovery of the GHASH authentication key through the Joux forbidden attack, allowing forged AES-GCM messages and injection of malicious responses. The response-counter check also fails to maintain last_response_counter, weakening replay and ordering validation. This issue is fixed in version 1.3.0.			
fbeta-GmbH--ePA3-Service-OpenSource	ePA 3.x Integration implements the authorization workflow and writes Medical Information Objects to Germany's electronic patient record. Prior to 1.3.0, ePA 3.x Integration disables TLS certificate verification for both ePA connections in app/vau/VAUProtokoll.py and Konnektor connections in app/konnektor/Konnektor.py. A network-positioned attacker can present an arbitrary certificate, terminate the TLS connection, and intercept ePA traffic. The VAU protocol does not provide an effective fallback because its application-layer certificate validation is also broken in affected versions. The Konnektor session uses self.session.verify set to False while the client authenticates with self.session.cert, so an attacker impersonating the Konnektor can receive the client's mutual TLS certificate exchange and observe smartcard operations. This issue is fixed in version 1.3.0.	2026-08-18	7.5	CVE-2026-50578
FFmpeg--FFmpeg	FFmpeg before commit 1c10bcc contains a heap buffer overflow in the RIST protocol reader (libavformat/librist.c). librist_read() ignored its size argument and copied the full received payload length into the caller-provided destination buffer, overflowing it when the payload exceeds the destination size. This is reachable via the async:rism:// URL scheme, where the async wrapper supplies a smaller buffer than the received payload. A remote RIST sender can trigger the overflow by sending a packet whose payload exceeds the caller buffer size.	2026-08-19	9.8	CVE-2026-75143
FFmpeg--FFmpeg	FFmpeg before commit 65b0dab contains an out-of-bounds read in the DASH demuxer (libavformat/dashdec.c). When a live DASH manifest is refreshed with a startNumber that is lower than the previous value, the current sequence number is driven negative. The fragment retrieval function checked only the upper bound before indexing the fragments array, allowing a negative index to be used and causing an out-of-bounds read. A malicious or misconfigured DASH server can trigger this by serving a live manifest with a decreasing startNumber across a manifest refresh.	2026-08-19	8.1	CVE-2026-75146
FFmpeg--FFmpeg	FFmpeg before commit acf5d7c contains a heap buffer overflow in the hvcC box writer. When writing an HEVC configuration record with more NAL units of a single type than the count field can represent, the NAL unit count overflows, causing a heap buffer overflow. A crafted HEVC input file triggers the overflow during muxing.	2026-08-19	7.8	CVE-2026-75141
FFmpeg--FFmpeg	FFmpeg before commit 9d786e4 contains a stack buffer overflow in the MPEG-PS muxer (libavformat/mpegenc.c). When muxing input with more streams than the muxer's fixed-size stack buffer accommodates, the buffer is overflowed. A crafted input with an excessive number of streams triggers the overflow during MPEG-PS muxing.	2026-08-19	7.8	CVE-2026-75142
FFmpeg--FFmpeg	FFmpeg before commit 1cdeb3c contains a heap buffer overflow vulnerability in the VC-2/Dirac RTP packetizer (libavformat/rtpenc_vc2hq.c) that allows attackers to trigger memory corruption by supplying a crafted Dirac data unit. The packetizer copies an input-derived data unit or fragment size into a fixed-size buffer without an upper bound check, causing a heap buffer overflow when the crafted input is packetized for RTP output.	2026-08-19	7.8	CVE-2026-75144
FFmpeg--FFmpeg	FFmpeg before commit 983dae9 contains an out-of-bounds read in the AV1 RTP packetizer (libavformat/rtpenc_av1.c). The keyframe detection loop that searches for a sequence header OBU advanced its pointer and remaining-size counter by the encoded header length plus the OBU payload size without first bounding the OBU size against the remaining data. A crafted OBU size causes the remaining-size counter to wrap to a positive value, causing the next loop iteration to dereference a pointer beyond the end of the packet buffer. A crafted AV1 input packet muxed to RTP triggers the out-of-bounds read.	2026-08-19	7.1	CVE-2026-75147
frangoteam--FUXA	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. Prior to 1.3.2, the DEVICE_WEBAPI_REQUEST and DEVICE_PROPERTY Socket.IO handlers in server/runtime/index.js omit isSocketWriteAuthorized and accept attacker-controlled property.address or endpoint connection data. A remote unauthenticated attacker can make server/runtime/devices/httprequest/index.js call axios.get against arbitrary HTTP or HTTPS destinations, connect to reachable OPC UA or ODBC services, and receive results through the corresponding Socket.IO event. This read SSRF oracle can expose cloud instance metadata, internal	2026-08-18	8.2	CVE-2026-47719

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	administrative services, industrial endpoints, and ODBC data reachable from the FUXA host, including when secureEnabled is true. This issue is fixed in version 1.3.2.			
frappe--erpnext	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.111.0 and 16.22.0, limited authenticated users can cross a permission boundary in Frappe safe execution because frappe.render_template is exposed without forcing restrict_globals, allowing server-side template injection and remote code execution. This issue is fixed in versions 15.111.0 and 16.22.0.	2026-08-17	9.9	CVE-2026-65974
frappe--erpnext	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.116.0 and 16.23.0, erpnext/selling/report/inactive_customers/inactive_customers.py accepts an unvalidated doctype filter and interpolates it into raw SQL in get_sales_details and get_last_sales_amt, allowing an authenticated user to extract sensitive information and manipulate database queries. This issue is fixed in versions 15.116.0 and 16.23.0.	2026-08-17	7.6	CVE-2026-65822
Frauscher Sensortechnik--FDS 102	An unauthenticated remote attacker in possession of a valid session identifier is able to continue using the session after it should have expired. This increases the risk associated with stolen, leaked, shared, or unattended sessions and may enable unauthorized continued access to the FDS web interface.	2026-08-20	9.8	CVE-2026-14950
Frauscher Sensortechnik--FDS 102	A low privileged remote attacker can hijack an active administrative session without needing to know the administrator password by extracting live plaintext session identifiers for authenticated users from downloadable error log archives.	2026-08-20	8.8	CVE-2026-14948
Frauscher Sensortechnik--FDS 102	An low privileged remote attacker can cause authenticated users to perform unintended actions in the FDS Web interface using malicious web pages.	2026-08-20	8	CVE-2026-14951
Frauscher Sensortechnik--FDS 102	A high privileged remote attacker can upload a .php file and then request it directly from /uploads/<filename>.php to achieve arbitrary code execution due to improper file type validation which could result in full system compromise.	2026-08-20	7.2	CVE-2026-14946
Frauscher Sensortechnik--FDS 102	A high-privileged remote attacker can upload malicious ZIP archive containing directory traversal sequences such as ../ can escape the intended extraction directory and write files to arbitrary locations on the server, potentially achieve arbitrary code execution due to improper validation of archive entry paths before writing files to disk which could result in full system compromise.	2026-08-20	7.2	CVE-2026-14947
Frauscher Sensortechnik--FDS 102	An unauthenticated remote attacker can retrieve sensible files from the FDS Web server, such as the backup archive at /FdsBackup.zip and additional files under /downloads/*, directly over HTTP without a valid session. These files disclose detailed railway signaling and track layout information that should not be available to unauthenticated users.	2026-08-20	7.5	CVE-2026-14952
FreeCAD--FreeCAD	FreeCAD is a free and open-source multiplatform 3D parametric modeler. From 0.19 until 1.1.1, src/Mod/BIM/bimcommands/BimProjectManager.py in the BIM Project Manager Load Template flow passes attacker-controlled FCStd Meta property values for wposition, wpu, wpv, and wpaxis directly to eval(), allowing arbitrary Python code execution when a user loads a malicious BIM project template. This issue is fixed in version 1.1.1.	2026-08-17	7.8	CVE-2026-34398
FreeCAD--FreeCAD	FreeCAD is a free and open-source multiplatform 3D parametric modeler. From 0.19 until 1.1.1, FreeCAD's BIM Workbench contains an eval() call on untrusted data from SVG template files. When a user creates a TechDraw page from a malicious SVG template, arbitrary Python code executes. The vulnerable code is in src/Mod/BIM/bimcommands/BimTDPPage.py (line 87). This issue is fixed in version 1.1.1.	2026-08-17	7.8	CVE-2026-34399
FreeCAD--FreeCAD	FreeCAD is a free and open-source multiplatform 3D parametric modeler. Prior to 1.1.2, src/App/PropertyPythonObject.cpp in PropertyPythonObject::Restore() passes the attacker-controlled module attribute from serialized PropertyPythonObject XML directly to PyImport_ImportModule() while restoring a crafted FCStd document, which executes module-level Python code, and the legacy pickle branch also imports an attacker-controlled module and invokes its class constructor through PyObject_CallObject(). This issue is fixed in version 1.1.2.	2026-08-17	7	CVE-2026-34789
FreeRTOS--FreeRTOS-Kernel	Improper input validation in FreeRTOS-Kernel before 11.3.1 might allow an unprivileged task on MPU-enabled ports to execute code in privileged kernel context. To remediate this issue, users should upgrade to version 11.3.1 or later.	2026-08-21	8.8	CVE-2026-77234
FreeRTOS--FreeRTOS-Kernel	Missing privilege verification in the secure context cleanup handler in FreeRTOS-Kernel before 11.3.1 might allow local users to cause a use-after-free condition in secure-world memory via the SVC handler for secure context deallocation. To remediate this issue, users should upgrade to version 11.3.1 or later.	2026-08-21	7.3	CVE-2026-77235

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
FreeRTOS--FreeRTOS-Kernel	Missing minimum size validation in secure context allocation in FreeRTOS-Kernel before 11.3.1 might allow local users to corrupt secure-world heap metadata via an out-of-bounds write with an undersized stack size parameter. To remediate this issue, users should upgrade to version 11.3.1 or later.	2026-08-21	7.3	CVE-2026-77236
froxlor--froxlor	Froxlor is open source server administration software. From 2.3.7 until 2.3.8, the Customers.get, Customers.listing, Admins.get, Admins.listing, Ftps.get, and Ftps.listing API commands in lib/Froxlor/Api/Commands/Customers.php, lib/Froxlor/Api/Commands/Admins.php, and lib/Froxlor/Api/Commands/Ftps.php retrieve full database rows and return them without removing password and data_2fa fields. An authenticated API caller with permission to use these endpoints can obtain customer, administrator, and FTP password hashes as well as Base32-encoded TOTP seeds for administrator and customer accounts. Password hashes can be cracked offline, and TOTP seeds can generate valid second-factor codes until two-factor authentication is reset. Exposure of both values for an account can enable takeover of the hosting panel or hosted resources and can defeat both authentication factors. This issue is fixed in version 2.3.8.	2026-08-18	9	CVE-2026-62988
froxlor--froxlor	Froxlor is open source server administration software. Prior to 2.3.7, the API authentication path in lib/Froxlor/Api/FroxlorRPC.php and FroxlorRPC::validateAuth accepts an API key and secret for an administrator or customer account without checking type_2fa, validating a TOTP code, or invoking FroxlorTwoFactorAuth. The web interface requires a second factor for accounts with two-factor authentication enabled, but the API grants access after validating only the API credentials, expiration, API permission, and account status. An attacker who obtains an API key and secret for a protected account can call the available API functions without supplying the configured second factor, which can expose or modify customer data, domains, email and FTP accounts, databases, DNS records, and certificate material. This issue is fixed in version 2.3.7.	2026-08-18	8.1	CVE-2026-52793
froxlor--froxlor	Froxlor is open source server administration software. Prior to 2.3.8, DNS TXT record content accepted by lib/Froxlor/Api/Commands/DomainZones.php can contain HTML special characters, lib/Froxlor/UI/Callbacks/Text.php returns the content from Text::wordwrap without HTML escaping, and templates/Froxlor/table/table.html.twig renders the callback result with the raw filter. An authenticated customer with DNS editor access can store JavaScript-bearing content in a TXT record. When an administrator views the affected domain's DNS configuration, the payload executes automatically in the administrator's browser session, which can expose session data or perform privileged panel actions. This issue is fixed in version 2.3.8.	2026-08-18	8.7	CVE-2026-54347
froxlor--froxlor	Froxlor is open source server administration software. Prior to 2.3.8, the Admins.add and Admins.update endpoints in lib/Froxlor/Api/Commands/Admins.php accept an attacker-controlled ipaddress array and store it as JSON in panel_admins.ip without enforcing numeric element types. When the poisoned account later calls IpsAndPorts.listing, lib/Froxlor/Api/Commands/IpsAndPorts.php decodes the array and concatenates its elements into a SQL IN clause without casting or parameterization; the same unsafe pattern is present in lib/Froxlor/Api/Commands/Domains.php. An authenticated administrator with change_serversettings permission can store a UNION-based payload and trigger it through the poisoned account to retrieve arbitrary database data, including administrator login names and bcrypt password hashes, with potential privilege escalation and broader database impact. This issue is fixed in version 2.3.8.	2026-08-18	7.2	CVE-2026-54348
funstory-ai--BabelDOC	BabelDOC is a document translation tool. Prior to 0.6.3, BabelDOC's vendored PDF parser in babeldoc/pdfminer/cmapdb.py deserializes untrusted pickle data when CMapDB._load_data() loads CMap files. PDF-controlled Encoding or CMapName values and embedded PostScript usecmap operators can reach this sink after path separators are decoded, while _normalize_cmap_name() removes only a leading slash. Absolute paths or traversal sequences can escape the trusted CMap directories through os.path.join(), select an attacker-writable .pickle.gz file, and cause pickle.loads() to execute arbitrary Python code with the privileges of the BabelDOC process. This issue is fixed in version 0.6.3.	2026-08-21	7.8	CVE-2026-54071
FuyaWeb Internet and Informatics Services--ArchitectPanel Web Admin Panel	Execution after redirect (EAR) vulnerability in FuyaWeb Internet and Informatics Services ArchitectPanel Web Admin Panel allows Authentication Bypass. This issue affects ArchitectPanel Web Admin Panel: through 28072026.	2026-08-21	7.5	CVE-2026-16323

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
g5theme--Essential Real Estate	Customer PHP Object Injection in Essential Real Estate <= 5.3.3 versions.	2026-08-18	8.8	CVE-2026-32465
Gemini Labs--Site Reviews	Unauthenticated Cross Site Scripting (XSS) in Site Reviews <= 8.2.0 versions.	2026-08-18	7.1	CVE-2026-73382
geotools--geotools	GeoTools is an open source Java library that provides tools for geospatial data. Starting in version 30.5 and prior to versions 33.6, 34.5, and 33.6, an SQL Injection Vulnerability is present when executing OGC Filters with PostGIS DataStore implementation: `jsonArrayContains` function; Requires PostGIS 12 or greater with a String or JSON field. For PostGIS 12 and greater `jsonArrayContains(<column>, <pointer>, <value>)` function writes `<value>` into generated SQL without escaping. Patches are available in versions 33.6, 34.5, and 33.6. No known workaround is available. To limit scope of SQL Injection the PostGIS connection pool should be configured with limited rights.	2026-08-21	9.8	CVE-2026-76904
Get Maps Marker Pro--Maps Marker Pro	Unauthenticated SQL Injection in Maps Marker Pro <= 4.32 versions.	2026-08-19	9.3	CVE-2026-73183
getgrav--grav	Grav before 2.0.14 fails to guard the access field in the core group blueprint with the required security@: admin.super restriction. A delegated admin.users operator can save a group with access[admin][super]=true to escalate to super-admin, gaining scheduler and Twig evaluation capabilities.	2026-08-18	9.1	CVE-2026-75837
getgrav--grav	Grav before 2.0.15 contains an arbitrary file write vulnerability in the Blueprint dynamic-data bare-function validation that uses an incomplete denylist instead of a positive allowlist. Attackers with page-edit or blueprint-config access can invoke the error_log function through a data directive to append PHP payloads to web-accessible files, achieving remote code execution.	2026-08-18	8.8	CVE-2026-75827
getgrav--grav	Grav before 2.0.15 contains a stored cross-site scripting vulnerability in the detectXss() function where unpaired quotes in unquoted attribute values bypass event-handler detection. Authenticated editors can inject event handlers like onerror= that pass validation and execute in visitor browsers when page content is rendered.	2026-08-18	8.7	CVE-2026-75828
getgrav--grav	grav-plugin-api versions before 1.0.15 fail to validate Twig content in the translate() endpoint, allowing attackers with api.pages.write permission to persist pages with process.twig enabled. Attackers can submit crafted header and content parameters to execute server-side template injection payloads that are evaluated at render time.	2026-08-18	8.1	CVE-2026-75829
getgrav--grav	The Grav API plugin (getgrav/grav-plugin-api, bundled with Grav's admin-next/API stack) before 1.0.14 fails to enforce the authorize requirement in MenuBarController::executeAction(). While the GET /menubar/items listing endpoint correctly filters menubar items via userPassesAuthorize(), the POST /api/v1/menubar/actions/{plugin}/{action} endpoint only checks the baseline api.access permission and never evaluates the authorize field a plugin registered for that action. Any authenticated caller with api.access can therefore invoke a privileged menubar action directly, bypassing the intended authorization. No plugin bundled with core Grav currently registers a privileged authorize handler, so on a stock install the impact is latent; the flaw affects any first- or third-party plugin relying on the documented authorize semantics.	2026-08-18	8.8	CVE-2026-75836
getgrav--grav	Grav Login Plugin adds login, basic ACL, and session wide messages to Grav. Prior to 3.8.11, the Grav Login plugin login.regenerate2FASecret task checks only that the pending-session user exists rather than requiring \$user->authorized. After submitting a victim's correct password, an attacker can invoke taskRegenerate2FASecret() during the pending TOTP challenge, overwrite twofa_secret, read the replacement secret from the response, calculate a valid code, and complete authentication without the victim's second factor. This issue is fixed in version 3.8.11.	2026-08-19	7.4	CVE-2026-62669
getgrav--grav	grav-plugin-api (getgrav/grav-plugin-api) versions >= 1.0.0-beta.10 and <= 1.0.14 contain a path traversal vulnerability in the PagesController::batchCopy() method. An incomplete fix for GHSA-qjq4-jp55-4mx2 left the user-controlled 'suffix' parameter (via POST /api/v1/pages/batch) unvalidated. An authenticated user with the api.pages.write permission (editor-level, not super-admin) can supply path traversal sequences (e.g. ../../../../) in the suffix parameter to escape the intended user/pages/ directory and write attacker-controlled page content and page media to arbitrary filesystem locations writable by the web server process. The vulnerability is fixed in 1.0.15.	2026-08-18	7.1	CVE-2026-75830

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getgrav--grav	Grav before 2.0.15 contains a stored cross-site scripting vulnerability in the audio and video media rendering through the sourceParsedownElement method. The media URL fragment is concatenated unescaped into rawHtml source elements, allowing attackers to inject arbitrary HTML and JavaScript that executes in viewers' sessions.	2026-08-18	7.6	CVE-2026-75831
getgrav--grav-plugin-api	Grav API Plugin is a RESTful API for Grav CMS that provides full headless access to your site's content. Prior to 1.0.6, Grav API plugin UsersController::createApiKey(), generate2fa(), and disable2fa() omit the accessGrantsSuper() target check used by sibling user mutation endpoints. A non-super account with api.users.write can mint an API key bound to an access.api.super target through requireApiKeyPermission(), obtain the target's full privileges because key scopes are not enforced, and create persistent super-administrator access; the same missing check also permits rotating or disabling the target's two-factor authentication. This issue is fixed in version 1.0.6.	2026-08-19	8.8	CVE-2026-62666
getgrav--grav-plugin-api	Grav API Plugin is a RESTful API for Grav CMS that provides full headless access to your site's content. Prior to 1.0.6, the Grav API plugin ApiKeyManager::generateKey() stores a declared scopes array, but ApiKeyAuthenticator::authenticate() does not read keyData[scopes] and returns the owning user's complete identity. AbstractApiController::requirePermission() consequently evaluates the full user ACL, so a key issued for a read-only scope can perform every write, delete, and administrative operation available to the owner. This issue is fixed in version 1.0.6.	2026-08-19	8.1	CVE-2026-62667
getgrav--grav-plugin-api	Grav API Plugin is a RESTful API for Grav CMS that provides full headless access to your site's content. Prior to 1.0.0-rc.16, the Grav API plugin CorsMiddleware returns Access-Control-Allow-Origin: * and permissive OPTIONS responses for authenticated /api/v1 endpoints. JavaScript from any origin can submit an attacker-obtained JWT through the Authorization or X-API-Token header, read the authenticated response, and perform write operations with the token owner's privileges, enabling data exfiltration and account modification. This issue is fixed in version 1.0.0-rc.16.	2026-08-19	8.2	CVE-2026-63407
getgrav--grav-plugin-api	Grav API Plugin is a RESTful API for Grav CMS that provides full headless access to your site's content. Prior to 1.0.0-rc.16, the Grav API plugin JwtAuthenticator::extractBearerToken() accepts a JWT from the token URL query parameter on every /api/v1 route, including state-changing endpoints. Request URLs consequently expose valid access tokens through Apache, proxy, and CDN logs, browser history, and Referer headers, allowing a party with access to those records to reuse the token with the owner's API privileges. This issue is fixed in version 1.0.0-rc.16.	2026-08-19	7.5	CVE-2026-63408
getkin--kin-openapi	kin-openapi is a Go project for handling OpenAPI files. From 0.10.0 until 0.141.0, openapi3filter.convertParseError in openapi3filter/validation_error_encoder.go dereferences e.Parameter.In without checking whether e.Parameter is nil. A malformed non-string scalar field in a multipart/form-data request body produces a nested ParseError with a nil RequestError.Parameter, and applications that render the validation error through openapi3filter.ConvertErrors or ValidationErrorEncoder panic. An unauthenticated client can repeatedly send such requests to deny service when the application lacks a recovery boundary. JSON request bodies and applications that do not use these error-rendering helpers are not affected. This issue is fixed in version 0.141.0.	2026-08-21	7.5	CVE-2026-76905
ggml-org--llama.cpp	llama.cpp before b8585 contains a use-after-free vulnerability in the RPC server's GRAPH_RECOMPUTE handler that allows unauthenticated remote attackers to achieve arbitrary read and write access by storing a computation graph, freeing referenced buffers, and reclaiming freed memory with attacker-controlled content. Attackers can send RPC requests to trigger re-execution of stored graphs with dangling pointers, enabling full remote code execution without requiring authentication or user interaction.	2026-08-21	8.1	CVE-2026-39909
ggml-org--llama.cpp	A vulnerability was found in ggml-org llama.cpp bec4772f6. The impacted element is the function deserialize_tensor of the file ggml/src/ggml-rpc/ggml-rpc.cpp of the component ggml-RPC Server. Performing a manipulation of the argument op/op_params results in deserialization. The attack may be initiated remotely. This vulnerability is distinct from CVE-2026-34159 (GHSAs-j8rj-fmpv-wcxw, PR #20908), which only added a buffer==nullptr rejection in create_node() and does not validate op or op_params. The reported GitHub issue was closed automatically due to inactivity.	2026-08-23	7.3	CVE-2026-78147

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gingerplugins--Sticky Chat Widget	Unauthenticated SQL Injection in Sticky Chat Widget <= 1.4.2 versions.	2026-08-18	9.3	CVE-2026-73187
git-for-windows--git	Git for Windows is the Windows port of Git. Prior to 2.55.0.windows.4, a malicious remote Git server can advertise a bundle URI that reaches transport_get_remote_bundle_uri(), fetch_bundle_uri_internal(), and copy_uri_to_file() in bundle-uri.c during clone or fetch when transfer.bundleuri=true. Non-HTTP(S) values are treated as local filesystem paths, and file URI prefixes are removed, so a bare UNC path or file URI targeting an attacker-controlled share causes Windows to initiate an outbound SMB connection. This can expose NTLM authentication material to the attacker-selected host. This issue is fixed in version 2.55.0.windows.4.	2026-08-21	7.4	CVE-2026-62960
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.11.11, 19.0 before 19.0.8, 19.1 before 19.1.6, and 19.2 before 19.2.4 that under certain conditions could allow an unauthenticated user to remotely modify or delete public projects and user data via a GraphQL directive.	2026-08-17	9.4	CVE-2026-19478
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.8 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user to achieve remote code execution due to a path traversal vulnerability in the package registry.	2026-08-23	8.5	CVE-2026-10053
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.2 before 18.11.11, 19.0 before 19.0.8, 19.1 before 19.1.6, and 19.2 before 19.2.4 that under certain conditions could have allowed an unauthenticated user to execute mutations via GET requests due to improper request validation in GraphQL multiplex query handling.	2026-08-17	7.1	CVE-2026-19650
gitpython-developers--GitPython	GitPython versions before 3.1.58 contain an arbitrary file overwrite vulnerability in IndexFile.from_tree, IndexFile.reset, and IndexFile.merge_tree methods that append caller-influenced treeish strings to git read-tree without option validation or argument separation. Attackers can inject the --index-output option to overwrite arbitrary files with a valid git-index blob, destroying existing file content at attacker-controlled writable paths.	2026-08-19	8.1	CVE-2026-76219
gitpython-developers--GitPython	GitPython before 3.1.58 contains a command execution vulnerability in the check_unsafe_options guard that can be bypassed by combining a single-character kwarg with split_single_char_options=False. Attackers can supply a crafted kwargs dictionary to guarded methods like clone_from to emit a joined token parsed as --upload-pack, enabling arbitrary OS command execution at default allow_unsafe_options=False.	2026-08-19	8.8	CVE-2026-76220
gitpython-developers--GitPython	GitPython before 3.1.58 contains a config-name injection vulnerability in the option-name validator that allows attackers to forge arbitrary git-config directives by injecting equals signs, hash symbols, and whitespace into option names. Attackers can inject malicious option names like 'sshCommand = touch /tmp/RCE #' to execute arbitrary commands via core.sshCommand or core.hooksPath on the next git operation.	2026-08-19	8.8	CVE-2026-76221
gitpython-developers--GitPython	GitPython before 3.1.58 fails to validate submodule names from .gitmodules files, allowing attackers to create Git repositories at arbitrary filesystem paths outside the intended clone directory. Attackers can craft malicious repositories with traversal sequences in submodule names that GitPython processes during submodule initialization, creating attacker-controlled Git repositories at escaped filesystem locations.	2026-08-19	8.2	CVE-2026-76222
gitpython-developers--GitPython	GitPython before 3.1.58 contains a remote code execution vulnerability in Repo.init that forwards unsafe git options without validation. Attackers can supply a template parameter pointing to a directory with malicious git hooks that execute arbitrary code when git operations are performed on the initialized repository.	2026-08-19	7.5	CVE-2026-76218
givanz--Vvweb	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.4, Vvweb backend digital asset operations allow a low-privileged Vendor to access digital assets linked to another Vendor's products. The admin/controller/product/digital-asset.php and admin/controller/product/digital-assets.php controllers and the admin/sql/sqlite/digital_asset.sql data queries use a caller-controlled digital_asset_id without consistently enforcing the current admin_id ownership boundary. An attacker can list assets, read asset names and file metadata, edit asset metadata, or delete asset records, which can disclose private product metadata, corrupt resource links, and cause data loss. This issue is fixed in version 1.0.8.4.	2026-08-18	8.8	CVE-2026-49221

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
givanz--Vvweb	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.4, Vvweb backend post revision operations allow a low-privileged Author to access revisions for posts owned by another Author. The admin/controller/content/revisions.php controller and admin/sql/sqlite/post_content_revision.sql queries trust caller-controlled post_id, language_id, and created_at values without consistently applying the current admin_id to revision lists, reads, restores, and deletes. An attacker can read historic post content, restore a revision over another Author's live post content, or delete revision records, exposing drafts, corrupting published content, and removing audit history. This issue is fixed in version 1.0.8.4.	2026-08-18	8.3	CVE-2026-49224
givanz--Vvweb	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.4, Vvweb backend product revision operations allow a low-privileged Vendor to access revisions for products owned by another Vendor. The admin/controller/product/revisions.php route reuses admin/controller/content/revisions.php, while admin/sql/sqlite/product_content_revision.sql trusts caller-controlled product_id, language_id, and created_at values without applying the current admin_id to revision reads, restores, and deletes. An attacker can read historic product content, restore a revision over another Vendor's live product content, or delete revision records, exposing private copy, corrupting product pages, and removing audit history. This issue is fixed in version 1.0.8.4.	2026-08-18	8.3	CVE-2026-49225
givanz--Vvweb	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.4, Vvweb backend post operations allow a low-privileged Author to access posts owned by another Author. The admin/controller/content/posts.php controller permits filter[admin_id] to replace the server-selected admin_id restriction and accepts a caller-controlled post_id for duplicate and delete actions, while admin/sql/sqlite/post.sql does not consistently enforce post.admin_id. An attacker can view post metadata, discover post identifiers, duplicate posts, or delete posts and related content, exposing private drafts and causing content pollution, data loss, or business disruption. This issue is fixed in version 1.0.8.4.	2026-08-18	8.3	CVE-2026-49226
givanz--Vvweb	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.4, Vvweb backend product operations allow a low-privileged Vendor to access products owned by another Vendor. The admin/controller/product/products.php controller accepts a caller-controlled product_id for duplicate and delete actions, and admin/sql/sqlite/product.sql loads and mutates products without consistently applying the current admin_id when view_other_products or edit_other_products is absent. An attacker can read product details, duplicate products, or delete products and related catalog data, exposing commercial information and causing unauthorized copies, catalog pollution, data loss, or business disruption. This issue is fixed in version 1.0.8.4.	2026-08-18	8.8	CVE-2026-49228
givanz--Vvweb	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.4, Vvweb backend product question operations allow a low-privileged Vendor to manage questions under another Vendor's products. The admin/sql/sqlite/product_question.sql queries accept a caller-controlled product_question_id and do not verify product_question.product_id against product.admin_id for the current admin_id. An attacker can read pending question content and moderation data, change question status, edit question content, or delete questions, manipulating product Q&A visibility and integrity. This issue is fixed in version 1.0.8.4.	2026-08-18	7.6	CVE-2026-49222
givanz--Vvweb	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.4, Vvweb backend product review operations allow a low-privileged Vendor to manage reviews under another Vendor's products. The admin/sql/sqlite/product_review.sql queries accept a caller-controlled product_review_id and do not verify product_review.product_id against product.admin_id for the current admin_id. An attacker can read pending review content, ratings, author information, and moderation state, change review status, edit review content, or delete reviews, manipulating product review visibility and integrity. This issue is fixed in version 1.0.8.4.	2026-08-18	7.6	CVE-2026-49223
givanz--Vvweb	Vvweb is a powerful and easy to use CMS with page builder to build websites, blogs or ecommerce stores. Prior to 1.0.8.4, Vvweb backend comment operations allow a low-privileged Author to manage comments under another Author's posts. The admin/controller/content/comment.php and admin/controller/content/comments.php controllers and the	2026-08-18	7.6	CVE-2026-49227

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	admin/sql/sqlite/comment.sql queries accept a caller-controlled comment_id without verifying comment.post_id against post.admin_id for the current admin_id. An attacker can read pending comment content and commenter email addresses, change moderation status, edit comment content, or delete comments, breaking author and moderation boundaries. This issue is fixed in version 1.0.8.4.			
GL.iNet--A1300	A vulnerability was identified in GL.iNet A1300, AX1800, AXT1800, BE1400, BE3600, BE6500, BE9300, BE10000, E5800, MT2500, MT3000, MT3600BE, MT5000, MT6000, X2000, X3000 and XE3000 up to 4.8.x. Affected by this vulnerability is the function COPY/MOVE of the component WebDAV Service. Such manipulation leads to authorization bypass. It is possible to launch the attack remotely. The vendor explains: "After our investigation, we have confirmed that the vulnerability described (...) does indeed exist."	2026-08-17	8.3	CVE-2026-19979
GL.iNet--A1300	A vulnerability was detected in GL.iNet A1300, AX1800, AXT1800, MT2500, MT3000, MT6000, X3000 and XE3000 4.8.x. This issue affects some unknown processing of the file /usr/bin/gl_nas_sys of the component NAS Command Service. The manipulation results in os command injection. The attack may be launched remotely. Upgrading to version 4.9.0 is capable of addressing this issue. It is suggested to upgrade the affected component. The vendor explains: "After our investigation, we have confirmed that the vulnerability described (...) does indeed exist."	2026-08-17	8.3	CVE-2026-19983
GL.iNet--A1300	A security flaw has been discovered in GL.iNet A1300, AX1800, AXT1800, BE1400, BE3600, BE6500, BE9300, BE10000, E5800, MT2500, MT3000, MT3600BE, MT5000, MT6000, X2000, X3000 and XE3000 up to 4.8.x. Affected by this issue is the function ui.update_langs of the component Language Update. Performing a manipulation of the argument hour/min/week results in code injection. The attack can be initiated remotely. The vendor explains: "After our investigation, we have confirmed that the vulnerability described (...) does indeed exist."	2026-08-17	7.4	CVE-2026-19980
GL.iNet--A1300	A weakness has been identified in GL.iNet A1300, AX1800, AXT1800, BE1400, BE3600, BE6500, BE9300, BE10000, E5800, MT2500, MT3000, MT3600BE, MT5000, MT6000, X2000, X3000 and XE3000 up to 4.8.x. This affects an unknown part of the component Wi-Fi Timer Power-Schedule Feature. Executing a manipulation of the argument switch_power/restore_power can lead to os command injection. The attack can be launched remotely. The vendor explains: "After our investigation, we have confirmed that the vulnerability described (...) does indeed exist."	2026-08-17	7.4	CVE-2026-19981
GL.iNet--BE9300	A security vulnerability has been detected in GL.iNet BE9300 and MT6000 4.8.x. This vulnerability affects unknown code of the component Firewall-management RPC. The manipulation of the argument dest_port/dest_ip leads to os command injection. The attack may be initiated remotely. Upgrading to version 4.9.0 is able to resolve this issue. The affected component should be upgraded. The vendor explains: "After our investigation, we have confirmed that the vulnerability described (...) does indeed exist."	2026-08-17	7.4	CVE-2026-19982
GNU--Emacs	GNU Emacs before 31.0.91 contains an integer overflow in the PBM/PPM/PGM image loader that allows an attacker to leak heap memory contents by supplying a crafted image with large dimensions and an elevated max color index. The image loader multiplies image dimensions and channel count using signed integer arithmetic; for sufficiently large values, the result wraps to a negative number, bypassing the bounds check and causing the pixel reader to access heap memory past the end of the allocated buffer. The over-read contents are interpreted as pixel color values and rendered on screen.	2026-08-21	7.1	CVE-2026-77219
go-vikunja--vikunja	Vikunja through 2.4.0 contains a principal-type confusion vulnerability where LinkSharing principals with id N are treated as user principals with users.id == N at three permission checks lacking type guards. Attackers with a link-share JWT can remove victims from teams, enumerate and delete victim bot users, or read team rosters by exploiting id collisions in the autoincrement space.	2026-08-19	7.5	CVE-2026-76216
goauthentik--authentik	authentik is an open-source identity provider. Prior to 2026.2.6 and 2026.5.5, the Remote Access Control endpoint list returns every configured endpoint to any authenticated user regardless of which applications the user may access, and the response includes connection settings that can contain stored credentials. The endpoint listing does not apply the access controls governing the endpoints, and the connection flow does not confirm that an endpoint belongs to the Remote Access Control application through which it was launched. Any authenticated user can therefore read every endpoint together with its host and stored credentials and can open a connection to an endpoint belonging to another application. This exposes stored credentials for managed RDP, SSH, and VNC targets and grants	2026-08-18	8.8	CVE-2026-61574

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	interactive access to systems the user was never authorized to reach. Deployments that do not use the enterprise Remote Access Control provider are not affected. This issue is fixed in versions 2026.2.6 and 2026.5.5.			
gohugoio--hugo	Hugo 0.161.0 placed the Node asset pipelines behind the Node.js permission model so that code running through PostCSS, Babel, or TailwindCSS could not reach the file system outside the project directory. Hugo 0.162.0 added tailwindcss to the AllowChildProcess default in config/security/securityConfig.go, which makes nodePermissionArgs in common/hexec/exec.go append --allow-child-process whenever the tool being launched is named tailwindcss. TailwindCSS loads the site's tailwind.config.js through require at startup, so top-level code in that file executes inside the permitted Node process and can call child_process to spawn a shell. The spawned process is not a Node process and inherits none of the permission flags, so it runs with the full privileges of the account performing the build. Building a site whose theme, module, or starter template supplies the Tailwind configuration therefore yields arbitrary command execution rather than the confined file access the permission model was introduced to enforce. Hugo 0.165.0 removes tailwindcss from the default security.exec.allow list, so the tool is no longer launched under the default configuration.	2026-08-18	8.6	CVE-2026-75926
gotenberg--gotenberg	Gotenberg is a Docker-powered stateless API for PDF files. In 8.32.0 and earlier, filename handling in pkg/modules/api/context.go uses filepath.Base on Linux, which does not treat backslashes as path separators, so a multipart filename containing Windows-style parent directory components survives sanitization. The original filename flows through ctx.diskToOriginal and the multi-output PDF routes into archives.FilesFromDisk and archives.Zip.Archive as the generated zip entry name. A remote attacker can submit a name such as\\Windows\\System32\\evil.pdf through an upload or an upstream downloadFrom Content-Disposition header, and a Windows archive extractor can write the resulting file outside the intended extraction directory. The affected paths include /forms/pdfengines/split and other multi-output PDF, LibreOffice, and conversion routes, and exploitation can cause arbitrary file writes on a downstream Windows system when a user or process extracts the returned archive. This issue is fixed in version 8.33.0.	2026-08-19	8.8	CVE-2026-44829
gotenberg--gotenberg	Gotenberg is a Docker-powered stateless API for PDF files. In 8.32.0 and earlier, the IsPublicIP function in pkg/gotenberg/outbound.go does not reject the 2002::/16 6to4 prefix, the 64:ff9b::/96 and 64:ff9b:1::/48 NAT64 prefixes, the fec0::/10 deprecated site-local prefix, Teredo, and other transition prefixes that can embed or route to non-public IPv4 destinations. The addr.Unmap operation only handles IPv4-mapped IPv6 addresses, so a crafted DNS AAAA record can cause the outbound HTTP client to treat an address wrapping an internal destination such as 169.254.169.254 as public. An unauthenticated attacker can use a conversion route with WithDenyPrivateIPs enabled to reach cloud metadata services, and the Chromium URL conversion route can return the internal response as a PDF, potentially exposing cloud credentials. Exploitation requires a deployment whose host routes the relevant IPv6 prefix, such as a dual-stack or NAT64-enabled environment. This issue is fixed in version 8.33.0.	2026-08-19	7.5	CVE-2026-45741
gotenberg--gotenberg	Gotenberg is a Docker-powered stateless API for PDF files. From 8.10.0 until 8.33.0, the newContext function in pkg/modules/api/context.go starts one errgroup.Go goroutine for each multipart downloadFrom entry and allows those goroutines to concurrently write to the shared ctx.files, ctx.diskToOriginal, and ctx.filesByField maps and slices. Go maps and slices are not safe for concurrent mutation, so a crafted multipart request containing many downloadFrom entries can trigger a data race and terminate the process with a fatal concurrent map writes runtime error. The default configuration enables downloadFrom and disables authentication, allowing an unauthenticated remote attacker to crash an exposed conversion service and cause a denial of service. This issue is fixed in version 8.33.0.	2026-08-19	7.5	CVE-2026-45742
Grafana--Grafana OSS	An authenticated user with permission to create or edit alert rules can bypass datasource query authorization by marking an alert rule query as a server-side expression while referencing a real datasource UID (incorrect authorization). This can expose data accessible through Grafana's configured datasource credentials to users who lack permission to query that datasource.	2026-08-19	7.1	CVE-2026-17183
gwin--WPAverts Classifieds Plugin	The WPAverts - Classifieds Plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.3.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This	2026-08-18	7.5	CVE-2026-11801

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	makes it possible for unauthenticated attackers to retrieve internal site configuration data exposed by the classifieds-types REST endpoint, including registered post types, labels, associated taxonomies, form scheme metadata, contact options, and custom field meta keys.			
hank-ai--darknet	hank-ai/darknet sizes a convolutional layer's weight and output heap buffers by multiplying configuration fields taken from a .cfg file in unchecked 32-bit int arithmetic. In src-lib/convolutional_layer.cpp, l.nweights is computed as (c / groups) * n * size * size and l.outputs as l.out_h * l.out_w * l.out_c, and both feed xmalloc directly. A .cfg whose true dimension product exceeds INT_MAX wraps to a small or zero value, so the allocation is undersized; for example width and height of 256 with filters of 65536 gives 2^32, which wraps to 0. forward_convolutional_layer then re-derives the GEMM dimensions with a different operand order, computing k as l.size*l.size*l.c / l.groups where the allocation divided before multiplying, and reads and writes through the undersized buffer. Loading the crafted .cfg for inference or training is sufficient and no valid .weights file is required. The reported proof of concept observed a heap buffer overflow read in gemm_nn_fast under AddressSanitizer and glibc allocator metadata corruption in a release build of the same input, indicating an out-of-bounds write.	2026-08-20	7.8	CVE-2026-72852
harttle--liquidjs	LiquidJS is a Shopify / GitHub Pages compatible template engine in pure JavaScript. Prior to 10.27.2, the join filter in src/filters/array.ts computes complexity from array.length and separator length instead of the total string length produced by array.join(sep). The concat filter can cheaply double arrays of references, after which join materializes the referenced content while charging only for element count, allowing a template to exceed a configured memoryLimit by a large factor. The sibling array_to_sentence_string filter in src/filters/string.ts has the same accounting defect, and a crafted template can allocate toward V8's string or process memory limit and crash the process. This issue is fixed in version 10.27.2.	2026-08-19	7.5	CVE-2026-69222
hashcat--hashcat	hashcat fails to restrict command-line options when parsing restore files, allowing attackers to inject output-redirecting options like --outfile and --potfile-path. Attackers can craft restore files with malicious options to append attacker-controlled content to arbitrary files, enabling code execution when targeting shell startup files.	2026-08-22	7.8	CVE-2026-68766
HashiCorp--Packer	Packer up to 1.15.4 is vulnerable to an issue in the third-party plugin installer that may allow unintended file system modification and could lead to code execution. A user who installs a plugin from a malicious or compromised source may be affected. This vulnerability (CVE-2026-19589) is fixed in Packer 1.16.0.	2026-08-17	7.1	CVE-2026-19589
HashThemes--Easy Elementor Addons	Cross-Site Request Forgery (CSRF) vulnerability in HashThemes Easy Elementor Addons allows Cross Site Request Forgery. This issue affects Easy Elementor Addons: from n/a through 2.3.7.	2026-08-20	9.6	CVE-2026-28164
HasThemes--Swatchly WooCommerce Variation Swatches for Products	Unauthenticated Cross Site Scripting (XSS) in Swatchly - WooCommerce Variation Swatches for Products <= 1.4.13 versions.	2026-08-20	7.1	CVE-2026-66605
Headroom Labs--Headroom	Headroom's LLM proxy derives the memory owner from the x-headroom-user-id request header. The header is read directly at several points in headroom/proxy/handlers/openai.py, including the chat completion and websocket paths, and nothing binds the value to the caller. A client can therefore name another user's identifier and read or write that user's stored LLM memory. The fix introduces a single resolve_memory_identity seam in headroom/proxy/identity.py that honors the header only for loopback or allowlisted callers and otherwise binds the identity to the proxy-token fingerprint or the operating system user. The pip console script binds 127.0.0.1 by default, but the reference docker-compose.yml ships --host 0.0.0.0 with published ports and no required HEADROOM_PROXY_TOKEN, which the server itself warns about at startup, so a deployment following the shipped compose exposes the affected data-plane routes to the network without authentication.	2026-08-21	9.1	CVE-2026-77776
Headroom Labs--Headroom	Headroom's LLM proxy lets a client choose the upstream destination with the x-headroom-base-url request header. _resolve_openai_upstream_base in headroom/proxy/handlers/openai.py accepts the header value, requires only that it parse with an http or https scheme and a hostname, and returns it for use as the upstream base; _select_passthrough_base_url in headroom/providers/proxy_routes.py reads the same header for the passthrough	2026-08-21	8.6	CVE-2026-77775

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	routes. No check rejects loopback, link-local, or RFC 1918 destinations, and because the component is a proxy the upstream response is returned to the caller, so the request reaches internal services and cloud metadata addresses and their responses are disclosed. The Authorization header accompanying the request is forwarded unchanged to the caller-designated host. The pip console script binds 127.0.0.1 by default, but the reference docker-compose.yml ships --host 0.0.0.0 with published ports and no required HEADROOM_PROXY_TOKEN, which the server itself warns about at startup, so a deployment following the shipped compose exposes the affected data-plane routes to the network without authentication.			
highwarden--Super Store Finder	Unauthenticated SQL Injection in Super Store Finder <= 7.8 versions.	2026-08-18	9.3	CVE-2026-73392
Hmbown--CodeWhale	CodeWhale (codewhale / codewhale-tui) versions >= 0.8.41 and < 0.8.64 contain an argument injection vulnerability in the git_show tool. The model-supplied rev parameter is passed unvalidated into the git show argv without an --end-of-options sentinel, so a value beginning with --output= is interpreted as a git flag. Because the tool is registered as auto-approved and advertised as read-only, an attacker (via a malicious repository combined with prompt injection) can cause an unprompted arbitrary file write at the privilege of the invoking user, targeting sensitive files such as ~/.ssh/authorized_keys, ~/.bashrc, or ~/.gitconfig. Fixed in 0.8.64 by adding rev validation.	2026-08-18	9.3	CVE-2026-75913
Hmbown--CodeWhale	CodeWhale before 0.8.64 contains a server-side request forgery bypass vulnerability in DNS pinning logic that fails to prevent time-of-check-time-of-use attacks. Attackers can manipulate DNS responses to fail initial resolution checks and succeed on secondary requests, allowing requests to internal IP addresses and bypassing SSRF mitigations.	2026-08-18	8.6	CVE-2026-75856
Hmbown--CodeWhale	CodeWhale versions >= 0.8.41 and < 0.8.64 contain a vulnerability in the exec_shell_interact (alias exec_interact) tool, whose approval_requirement returns ApprovalRequirement::Auto. This overrides the default Required approval for code-executing tools, so LLM-controlled stdin is written into an already-approved long-running interactive shell (e.g., a python3 -i REPL, mysql, ssh, or sudo -i session) without any approval prompt. An attacker who can inject instructions via untrusted content the agent ingests (a fetched page, MCP result, or repo file) can cause commands to run at the privilege level of that approved process. Fixed in 0.8.64.	2026-08-18	7	CVE-2026-75857
Hmbown--CodeWhale	CodeWhale (packages codewhale / codewhale-tui) versions >= 0.8.41 and < 0.8.64 contain a remote code execution vulnerability in the rlm_eval tool. The tool's approval_requirement() returns ApprovalRequirement::Auto, which the engine treats as 'never prompt,' causing arbitrary model-supplied Python code to run in a python3 interpreter without consulting the user's configured --approval-policy and without any approval prompt or audit step. An attacker can induce the agent to execute arbitrary code via prompt injection in untrusted content the agent reads (a web page, fetched URL, repository file, or MCP tool result); the companion rlm_open tool can stage such content. Code runs on the user's machine at the user's privilege level. Fixed in 0.8.64.	2026-08-18	7.8	CVE-2026-75858
Hmbown--CodeWhale	CodeWhale versions before 0.8.64 fail to validate file paths in the project config instructions field, allowing attackers to read arbitrary files on the victim's system. A malicious .codewhale/config.toml file in a cloned repository can specify paths outside the workspace that are read and injected into the AI system prompt for exfiltration.	2026-08-18	7.5	CVE-2026-75859
Hmbown--CodeWhale	CodeWhale versions before 0.8.64 fail to properly validate the allow_shell configuration parameter from project config files, allowing attackers to enable arbitrary shell command execution by committing a malicious .codewhale/config.toml file to a repository. When a user clones and opens the repository in CodeWhale, the AI model gains access to exec_shell and task_shell tools, enabling execution of arbitrary shell commands on the victim's machine without explicit user consent.	2026-08-18	7.8	CVE-2026-75911
Hmbown--CodeWhale	CodeWhale versions before 0.8.64 contain an argument injection vulnerability in the git_blame tool that allows attackers to read arbitrary files by injecting git options into the unvalidated rev parameter. Attackers can supply rev values like --contents=/path/to/file to exfiltrate sensitive files such as SSH keys and credentials through the tool output returned to the model.	2026-08-18	7.4	CVE-2026-75912
Hmbown--CodeWhale	CodeWhale versions before 0.8.64 contain a path traversal vulnerability in the image_analyze tool that fails to canonicalize symlinks before reading files.	2026-08-18	7.5	CVE-2026-75914

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Attackers can create workspace symlinks pointing to external files with image extensions to leak file bytes to the vision endpoint without user approval.			
Hmbown--CodeWhale	CodeWhale versions before 0.8.64 contain an environment variable exposure vulnerability in the js_execution tool that fails to scrub parent process environment variables before spawning Node.js. Attackers can craft malicious JavaScript code executed by the tool to read process.env and leak API keys, cloud credentials, and authentication tokens back to the model context.	2026-08-18	7.5	CVE-2026-75915
hoppscotch--hoppscotch	Hoppscotch is an open source API development ecosystem. Prior to 2026.6.0, the team, teamMembers.user, RESTHistory, GraphQLHistory, currentRESTSession, currentGraphQLSession, environments, globalEnvironments, and settings GraphQL paths expose another workspace member's private User data, while toggleHistoryStarStatus and removeRequestFromHistory in the UserHistory service accept another user's history identifier without enforcing userUid ownership, allowing an authenticated workspace member to read private request history, session data, request contents, authorization headers, environment values, and settings and to modify or delete the victim's private history entries. This issue is fixed in version 2026.6.0.	2026-08-18	7.6	CVE-2026-69189
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 NIM could allow a remote attacker to bypass security restrictions due to the exposure of intermediate certificate authority private keys in a publicly available update file.	2026-08-19	9.1	CVE-2026-15065
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 NIM could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-19	9.9	CVE-2026-15068
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to gain root privileges due to improper authentication.	2026-08-19	9.8	CVE-2026-16656
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-19	9.9	CVE-2026-16816
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to impersonate the TNC policy server and modify traffic due to improper certificate validation.	2026-08-19	9.3	CVE-2026-16822
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an integer underflow.	2026-08-19	9.8	CVE-2026-16834
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to obtain sensitive information due to an integer underflow in the IPv4 IP-options parser.	2026-08-19	9.4	CVE-2026-16839
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to an out-of-bounds write.	2026-08-19	9.8	CVE-2026-16840
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a heap buffer overflow.	2026-08-19	9.8	CVE-2026-16845
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack buffer overflow.	2026-08-19	9.8	CVE-2026-16862
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack buffer overflow.	2026-08-19	9.8	CVE-2026-16864
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack-based buffer overflow.	2026-08-19	9.8	CVE-2026-16872
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-19	9.8	CVE-2026-16882
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack buffer overflow.	2026-08-19	9.8	CVE-2026-16885
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack buffer overflow.	2026-08-19	9.8	CVE-2026-16894
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code or cause a denial of service due to an out-of-bounds write.	2026-08-19	9.6	CVE-2026-16903
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack buffer overflow.	2026-08-19	9.8	CVE-2026-16913
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to an integer overflow.	2026-08-19	9.8	CVE-2026-16917
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to improper validation of network-supplied pointers.	2026-08-19	9.8	CVE-2026-16919

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to overwrite arbitrary files due to improper neutralization of special elements in input.	2026-08-20	9.1	CVE-2026-16926
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	2026-08-20	9.8	CVE-2026-17040
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a use-after-free vulnerability.	2026-08-20	9.8	CVE-2026-17118
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack-based buffer overflow.	2026-08-20	9.8	CVE-2026-17122
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a format string vulnerability.	2026-08-20	9.8	CVE-2026-17136
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	2026-08-20	9.8	CVE-2026-17141
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary commands due to improper authentication.	2026-08-20	9.8	CVE-2026-17142
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to improper privilege management.	2026-08-20	9.8	CVE-2026-17145
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	2026-08-20	9.8	CVE-2026-17152
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack buffer overflow.	2026-08-20	9.8	CVE-2026-17157
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to an integer overflow during size computation.	2026-08-20	9.8	CVE-2026-17160
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to a buffer overflow.	2026-08-20	9.3	CVE-2026-17422
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-20	9.9	CVE-2026-18835
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 's nimesis registration service could allow a remote attacker to overwrite files due to path traversal.	2026-08-19	8.2	CVE-2026-15061
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 NIM could allow a remote attacker to gain unauthorized access to AIX systems due to improper validation of TLS certificates.	2026-08-19	8.1	CVE-2026-15078
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to access NFS-exported filesystems due to improper authentication.	2026-08-19	8.2	CVE-2026-16686
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a heap buffer overflow.	2026-08-19	8.8	CVE-2026-16814
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack buffer overflow.	2026-08-19	8.8	CVE-2026-16841
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-19	8.8	CVE-2026-16842
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-19	8.8	CVE-2026-16844
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a heap buffer overflow.	2026-08-19	8.8	CVE-2026-16847
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary commands due to improper neutralization of shell metacharacters in DHCP options.	2026-08-19	8.8	CVE-2026-16848
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to command injection via crafted Router Advertisements.	2026-08-19	8.8	CVE-2026-16850
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to manipulate network traffic and DNS configuration due to improper authentication.	2026-08-19	8.2	CVE-2026-16857
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to command injection.	2026-08-19	8.8	CVE-2026-16865
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote authenticated attacker to execute arbitrary code due to a stack-based buffer overflow.	2026-08-19	8.8	CVE-2026-16877
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to an out-of-bounds write.	2026-08-19	8.8	CVE-2026-16901

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to an off-by-one error in bounds checking.	2026-08-19	8.8	CVE-2026-16909
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote authenticated attacker to execute arbitrary code due to a stack buffer overflow.	2026-08-19	8.8	CVE-2026-16911
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary commands due to improper validation of the ODMDIR environment variable.	2026-08-20	8.8	CVE-2026-16932
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to a heap-based buffer overflow.	2026-08-20	8.8	CVE-2026-16934
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to a buffer overflow.	2026-08-20	8.8	CVE-2026-16936
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to a heap-based buffer overflow.	2026-08-20	8.2	CVE-2026-16943
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to an integer underflow.	2026-08-20	8.8	CVE-2026-16996
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to improper authentication.	2026-08-20	8.1	CVE-2026-17000
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a heap buffer overflow.	2026-08-20	8.3	CVE-2026-17006
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to obtain sensitive information and cause a denial of service due to a kernel heap over-read.	2026-08-20	8.1	CVE-2026-17060
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a stack-based buffer overflow.	2026-08-20	8.1	CVE-2026-17138
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote authenticated attacker to execute arbitrary code due to a stack-based buffer overflow.	2026-08-20	8.5	CVE-2026-17168
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a heap-based buffer overflow.	2026-08-20	8.8	CVE-2026-17436
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service and potentially disclose sensitive information due to an integer underflow.	2026-08-20	8.2	CVE-2026-18670
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote authenticated attacker to execute arbitrary commands due to improper neutralization of special elements used in an OS command.	2026-08-20	8.4	CVE-2026-18824
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a heap-based buffer overflow.	2026-08-20	8.8	CVE-2026-18832
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to improper validation of an attacker-controlled pointer.	2026-08-20	8.2	CVE-2026-18840
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to an out-of-bounds write.	2026-08-20	8.4	CVE-2026-18842
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to a buffer overflow.	2026-08-20	8.1	CVE-2026-19437
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 has a pointer validation flaw exists in the AIX Virtual SCSI (vSCSI) initiator driver. Successful exploitation may result in denial of service, privilege escalation, or full compromise of the client LPAR kernel.	2026-08-20	8.2	CVE-2026-19442
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 has a vulnerability in cmdnim that may allow an unprivileged local user to executes the payload as root.	2026-08-20	8.8	CVE-2026-19449
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 NIM server process is crashing during client registration due to buffer overflow.	2026-08-19	7.5	CVE-2026-14970
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to uncontrolled resource consumption.	2026-08-19	7.5	CVE-2026-16690
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to improper privilege management.	2026-08-19	7.8	CVE-2026-16703
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an out-of-bounds write.	2026-08-19	7.5	CVE-2026-16706
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a NULL pointer dereference.	2026-08-19	7.5	CVE-2026-16817
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to uncontrolled resource consumption.	2026-08-19	7.5	CVE-2026-16818

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service and compromise data integrity due to a time-of-check time-of-use race condition.	2026-08-19	7.7	CVE-2026-16819
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to unbounded recursion.	2026-08-19	7.5	CVE-2026-16824
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to uncontrolled resource consumption.	2026-08-19	7.5	CVE-2026-16831
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to uncontrolled resource consumption.	2026-08-19	7.5	CVE-2026-16836
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to improper handling of a missing SSL client certificate.	2026-08-19	7.5	CVE-2026-16837
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to overwrite critical files and obtain sensitive information due to a time-of-check to time-of-use (TOCTOU) race condition.	2026-08-19	7	CVE-2026-16838
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a use-after-free.	2026-08-19	7.4	CVE-2026-16851
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an integer overflow.	2026-08-19	7.5	CVE-2026-16852
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to improperly scrubbed environment variables.	2026-08-19	7.8	CVE-2026-16869
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to achieve local privilege escalation due to an out-of-bounds write.	2026-08-19	7.8	CVE-2026-16873
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to obtain root privileges due to improper enforcement of RBAC authentication roles.	2026-08-19	7.8	CVE-2026-16874
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary commands due to shell metacharacter injection.	2026-08-19	7.8	CVE-2026-16875
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to a time-of-check to time-of-use (TOCTOU) race condition.	2026-08-20	7	CVE-2026-16922
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to improper privilege management.	2026-08-20	7	CVE-2026-16923
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an improper calculation of a memory offset during IPsec decapsulation.	2026-08-20	7.5	CVE-2026-16924
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to achieve privilege escalation due to improper authorization.	2026-08-20	7.1	CVE-2026-16925
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain root privileges due to a time-of-check to time-of-use (TOCTOU) race condition.	2026-08-20	7.3	CVE-2026-16927
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a heap-based buffer overflow.	2026-08-20	7.5	CVE-2026-16928
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to a time-of-check to time-of-use (TOCTOU) race condition.	2026-08-20	7.8	CVE-2026-16935
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to improper privilege management.	2026-08-20	7.8	CVE-2026-16937
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to a stack-based buffer overflow.	2026-08-20	7.8	CVE-2026-16945
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to a heap buffer overflow.	2026-08-20	7.8	CVE-2026-16946
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to improper resolution of symbolic links.	2026-08-20	7.1	CVE-2026-16989
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to improper handling of symbolic links.	2026-08-20	7.8	CVE-2026-16991
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary commands due to improper privilege management.	2026-08-20	7.8	CVE-2026-16997
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to compromise the confidentiality and integrity of the system due to an out-of-bounds write.	2026-08-20	7.7	CVE-2026-17003
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to execute arbitrary code due to improper certificate validation.	2026-08-20	7.7	CVE-2026-17024
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to uncontrolled recursion.	2026-08-20	7.5	CVE-2026-17121

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to an out-of-bounds read.	2026-08-20	7.8	CVE-2026-17124
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an integer overflow.	2026-08-20	7.5	CVE-2026-17159
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to improper validation of an array size field.	2026-08-20	7.5	CVE-2026-17163
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a NULL pointer dereference.	2026-08-20	7.5	CVE-2026-17165
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to improper validation of an allocation size.	2026-08-20	7.5	CVE-2026-17170
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to overwrite arbitrary files due to improper resolution of symbolic links.	2026-08-20	7.8	CVE-2026-17171
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to obtain sensitive information and cause a denial of service due to an out-of-bounds read.	2026-08-20	7.7	CVE-2026-17423
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a stack buffer overflow.	2026-08-20	7.5	CVE-2026-17425
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote authenticated attacker to obtain sensitive information or cause a denial of service due to an out-of-bounds read.	2026-08-20	7.9	CVE-2026-18716
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 allows a remote unauthenticated attacker can send a crafted UDP packet to a reachable RPC service, resulting in complete system unavailability and requiring an LPAR restart.	2026-08-20	7.5	CVE-2026-19446
IBM--DS8A00 (R10.0 - R10.1)	IBM System Storage DS8A00 10.1.3.0 through 10.11.35.0 and IBM DS8900F 89.40.83.0 through 89.44.25.0 could allow an attacker to bypass security authentication due to improperly encoding of DSCSI command output to obtain sensitive information or cause a denial of service.	2026-08-19	7.4	CVE-2025-36254
IBM--DS8A00(R10.0 - R10.1)	IBM System Storage DS8A00 10.1.3.0 through 10.11.35.0 and IBM DS8900F 89.40.83.0 through 89.44.25.0 could allow an authenticated user to create a user with privileged user roles due to improper privileged defined with unsafe actions.	2026-08-19	7.5	CVE-2025-36255
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.0 could allow a remote attacker to overwrite administrator email information and abuse the server as an outbound relay due to missing authentication for the registration endpoint.	2026-08-19	7.5	CVE-2026-19875
IBM--Portieris	IBM Portieris 0.5.0 through 0.14.2 could allow a remote authenticated attacker to bypass image policy enforcement due to improper authorization of pod owner references.	2026-08-19	8.1	CVE-2026-18544
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the ASMI web interface. An unauthenticated attacker with network access can send the FSP a malformed request, allowing arbitrary code execution, giving the attacker full control over the managed system, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	9.6	CVE-2026-16687
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the FSP management network protocol. An unauthenticated attacker on the management network can bypass authentication and perform any administrative operation on the managed system, including control of partition power state, configuration, and console access across all hosted partitions, resulting in a confidentiality, integrity, and availability impact to the managed system.	2026-08-19	9.6	CVE-2026-16835
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the FSP management network protocol. An attacker with authenticated HMC administrator access can execute arbitrary code on the service processor, giving full control over the managed system, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	8.4	CVE-2026-16832
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, and FW1060.00 through FW1060.80 is affected by a vulnerability in the interface between the BMC/FSP and the host system. An attacker with service account or root access to the BMC/FSP can execute arbitrary code on the host system, giving full control over the host system and all hosted partitions, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	8.2	CVE-2026-16930
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, FW950.00 through FW950.H2, OP940.00 through	2026-08-19	8.2	CVE-2026-16933

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	OP940.a1 (Power9), and OP940.00 through OP940.81 (Power HMC) is affected by a vulnerability in the interface between the BMC/FSP and the host system. An attacker with service account or root access to the BMC/FSP can read and write arbitrary regions of host system memory, giving full control over the host system and all hosted partitions, resulting in a confidentiality, integrity, and availability impact.			
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, FW950.00 through FW950.H2, OP940.00 through OP940.a1 (Power9), and OP940.00 - OP940.81 (Power HMC) is affected by a vulnerability in host firmware configuration parsing. An attacker with service-level access to the BMC/FSP can supply specially crafted configuration data, compromising the host firmware boot stage and everything subsequently loaded by it, resulting in a confidentiality, integrity, and availability impact to the managed system.	2026-08-19	8.2	CVE-2026-17093
IBM--Power Systems Firmware	Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, FW950.00 through FW950.H2, OP940.00 through OP940.a1, and OP940.00 - OP940.81 is affected by a vulnerability in the service processor mailbox interface. An attacker with authenticated service-level access to the BMC/FSP can exploit this vulnerability, allowing arbitrary code to be executed in the host firmware runtime, giving full control over the managed system, resulting in a confidentiality, integrity, and availability impact to the managed system.	2026-08-19	8.2	CVE-2026-17100
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, FW950.00 through FW950.H2, OP940.00 through OP940.a1 (Power9), and OP940.00 - OP940.81 (Power HMC) is affected by a vulnerability in the interface between the BMC/FSP and the host system. An attacker with service account or root access to the BMC/FSP can write arbitrary data to hardware control registers, allowing full control over the host system and all hosted partitions, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	8.1	CVE-2026-17429
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, and FW1110.00 through FW1110.30 is affected by a vulnerability in the interface between the BMC and the host system. An attacker with service access to the BMC can send a specially crafted command, allowing arbitrary code to be executed on the host system, giving full control over the host system and all hosted partitions, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	8.2	CVE-2026-17494
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the ASMI web interface. An attacker who can lure a logged-in ASMI administrator to visit a crafted web page can, under specific conditions, silently perform administrative actions on the FSP on behalf of that administrator, resulting in a confidentiality, integrity, and availability impact to the managed system.	2026-08-19	8.3	CVE-2026-18848
IBM--Power Systems Firmware	Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, and FW1060.00 through FW1060.80 is affected by a vulnerability in the host firmware boot process image validation path. An attacker with service access to the service processor can supply a maliciously crafted code update image, allowing arbitrary code to be executed on the host system. Successful exploitation could result in a confidentiality, integrity, and availability impact to the affected host system.	2026-08-19	8.2	CVE-2026-19234
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the ASMI web interface. An unauthenticated attacker on the management network can cause the ASMI web server to crash with possible memory corruption and generate an error log; hosted partitions are not affected. The ASMI web interface will restart automatically; however, repeated exploitation could result in a sustained loss of access to the ASMI management interface, resulting in an integrity and availability impact.	2026-08-19	7.6	CVE-2026-16828
IBM--Power Systems Firmware	IBM Power Systems Firmware FW950.00 through FW950.H2, OP940.00 through OP940.a1 (Power9), and OP940.00 - OP940.81 (Power HMC) is affected by a vulnerability in host firmware NVRAM parsing. An attacker with root access to a guest partition on an OpenPOWER system can write a specially crafted NVRAM image, causing the host firmware boot stage to crash with possible memory corruption. This condition persists until operator intervention - clearing NVRAM via the service processor - to restore normal operation. This vulnerability only affects OpenPOWER systems; systems running PowerVM are not affected. Successful exploitation results in an integrity and availability impact to the managed system.	2026-08-19	7.3	CVE-2026-17042

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, and FW1060.00 through FW1060.80 is affected by a vulnerability in the interface between the BMC/FSP and the host system. An attacker with service account or root access to the BMC/FSP can access and disrupt host processor state, potentially affecting the managed system and all hosted partitions, resulting in a confidentiality, and availability impact.	2026-08-19	7.9	CVE-2026-17063
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the service processor mailbox interface. An attacker with authenticated service-level access to the FSP can exploit this vulnerability, allowing arbitrary code to be executed in the host firmware runtime, giving full control over the managed system, resulting in a confidentiality, integrity, and availability impact to the managed system.	2026-08-19	8.2	CVE-2026-16661
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the service processor mailbox interface. An attacker with authenticated service-level access to the FSP can send a specially crafted mailbox message to read or modify arbitrary regions of Hostboot memory, compromising the host firmware boot stack and the hypervisor subsequently loaded by it. Successful exploitation results in a confidentiality, integrity, and availability impact to the managed system.	2026-08-19	8.2	CVE-2026-16707
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the PowerVM hypervisor call interface. An attacker with root access to a guest partition can issue a specially crafted hypervisor call to inject an arbitrary amount of data into hypervisor or partition memory, resulting in either a crash causing a full platform re-IPL and terminating all hosted partitions, or corruption of hypervisor or partition memory. The PowerVM hypervisor will restart automatically; however, repeated exploitation could result in a sustained availability impact. Successful exploitation results in an integrity and availability impact to the managed system.	2026-08-19	8.4	CVE-2026-17091
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 Power Systems Firmware is affected by a vulnerability in partition firmware during network boot. An unauthenticated attacker with access to the same network as a partition performing a network boot can prevent that partition from completing its boot sequence. On partitions where OS secure boot is not enabled, which is the default configuration, the attacker can also substitute the boot image, compromising everything subsequently loaded by that partition. Other partitions and the managed system are not affected. Only partitions actively performing a network boot are affected, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	8.1	CVE-2026-17414
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the PowerVM hypervisor call interface. An attacker with root access to a guest partition can issue a specially crafted hypervisor call causing a virtual processor to become permanently unresponsive, requiring a full platform re-IPL to restore normal operation. In some cases this may also cause the guest to inject a small amount of data into hypervisor or partition memory with no attacker control over the target location. Successful exploitation results in an integrity and availability impact to the managed system.	2026-08-19	7.3	CVE-2026-17097
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 Power Systems Firmware is affected by a vulnerability in partition firmware during network boot. An unauthenticated attacker on the same network as a partition undergoing network boot can send a malformed packet, allowing arbitrary code to be executed in the partition firmware and compromising everything subsequently loaded by that partition. Other partitions and the managed system are not affected. Only partitions actively performing a network boot are affected, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	7.5	CVE-2026-18821
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, and FW1060.00 through FW1060.80 is affected by a vulnerability in host firmware configuration parsing. An attacker with authenticated service-level access to the service processor can write specially crafted configuration data, causing the host firmware boot stack to crash with possible memory corruption during system	2026-08-19	7.3	CVE-2026-18871

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	initialisation, resulting in an integrity and availability impact to the managed system.			
ICEcoder--ICEcoder	ICEcoder 8.1 contains an unauthenticated remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary OS commands by chaining an authentication bypass, CSRF validation bypass, and unsanitized command execution. Attackers can send a single HTTP POST request to the terminal endpoint with a password parameter to bypass authentication, a non-empty csrf parameter to skip CSRF validation, and an arbitrary command string passed directly to proc_open() to achieve remote code execution as the web-server user.	2026-08-19	9.8	CVE-2026-63722
indilib--indi	INDI (Instrument Neutral Distributed Interface) indiserver through 2.2.4.2, fixed in commit 96bbd7f, contains a stack buffer overflow vulnerability that allows unauthenticated remote attackers to crash the daemon by sending malformed XML with mismatched tags whose names exceed 1024 bytes. Attackers can send a single TCP packet on port 7624 with mismatched XML tags to trigger an unbounded sprintf() write into a fixed 1024-byte stack buffer in MsgQueue.cpp, terminating the daemon and disrupting all active client and driver sessions.	2026-08-17	7.5	CVE-2026-71979
indithemes--IT Residence	Subscriber Arbitrary File Upload in IT Residence <= 3.2.1 versions.	2026-08-20	9.9	CVE-2026-74014
infiniflow--ragflow	RAGFlow before 0.26.3 contains a server-side request forgery vulnerability in the agent workflow "Invoke" component (agent/component/invoke.py). The component builds an outbound request URL from canvas configuration and runtime template variables and passes it to requests.get, requests.post, or requests.put without calling the shared assert_url_is_safe validator or pinning the resolved address, unlike the crawler, SearXNG, file-upload, and RSS fetch paths. A user who can create or trigger an agent can direct the server to fetch loopback, link-local, and RFC 1918 destinations, including cloud instance metadata endpoints and services co-located on the deployment network, and the response body is returned as the component output. Where an agent is configured to interpolate the chat query into the Invoke URL, the destination is chosen by whoever can send that query.	2026-08-18	8.5	CVE-2026-75898
Innotim Software Telecommunicatio ns and Consulting Trade Ltd. Co.-- Logsign SIEM	Insufficiently Protected Credentials vulnerability in Innotim Software Telecommunications and Consulting Trade Ltd. Co. Logsign SIEM allows Retrieve Embedded Sensitive Data. This issue affects Logsign SIEM: from 6.4.97 before 6.4.114.	2026-08-17	9	CVE-2026-14564
InternLM--lmdeploy	LMDeploy deserializes disaggregated-serving peer messages with pickle. The handle_zmq_rcv coroutine in lmdeploy/pytorch/disagg/conn/engine_conn.py reads peer-to-peer cache-free requests with recv_pyobj(), which deserializes the received bytes with pickle.loads(), and the isinstance check against DistServeCacheFreeRequest runs only after deserialization has already completed. The peer that supplies those bytes is caller-controlled: p2p_connect passes remote_engine_endpoint_info.zmq_address from the request body to connect() on the ZMQ PULL socket, and the POST /distserve/p2p_initialize and /distserve/p2p_connect endpoints in lmdeploy/serve/openai/api_server.py apply no authentication unless the server is started with api_keys, which defaults to None. A remote attacker can direct an engine to pull from a ZMQ endpoint under their control and execute arbitrary code in the engine process. Deployments that do not enable disaggregated serving are not affected, because the receive loop is only started once the migration backend accepts the connection.	2026-08-19	9.8	CVE-2026-76850
ispconfig--ispconfig3	ISPConfig contains an authenticated SQL injection vulnerability in the Remote API. The primary_id parameter passed to delete and update API methods is concatenated directly into SQL WHERE clauses without integer casting or parameterized query binding. The built-in SQL injection scanner does not block quote-free boolean payloads and does not reject requests in its default configuration. A remote API user holding any single low-privilege function permission can inject arbitrary SQL to delete or modify records across all tenants in the control panel database and extract arbitrary data via blind boolean inference, including password hashes and client records.	2026-08-19	8.8	CVE-2026-61518
jahllives--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain an arbitrary code execution vulnerability in the Whirlpool hash implementation that uses broad glob patterns to load .so modules without integrity verification. Attackers can place malicious .so files matching the whirlpool*py313*.so pattern in site-packages directories to achieve native code execution when the module is loaded.	2026-08-17	9.8	CVE-2026-74872

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 silently skip JSON schema validation when the jsonschema library is not installed, allowing malformed metadata to be accepted. Attackers can remove the jsonschema package or supply unknown metadata format versions to bypass all schema checks and process malicious data.	2026-08-17	9.8	CVE-2026-74875
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a vulnerability in PublicKeyBundle.from_dict() that creates key bundles from untrusted data without verifying signatures. Attackers can call from_dict() followed by to_identity() without signature verification to encrypt data using attacker-controlled public keys, leaking secrets.	2026-08-17	9.8	CVE-2026-74876
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 use an in-memory rate limiter for TOTP brute-force protection that is not shared across workers and is lost on server restart. Attackers can distribute authentication attempts across multiple server instances or retry immediately after a restart to bypass rate limiting protections.	2026-08-17	9.8	CVE-2026-74878
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 accept refresh tokens as URL query parameters in keyserver and telemetry server routes. Attackers can extract tokens from server logs, proxy logs, browser history, and HTTP Referer headers to gain unauthorized access.	2026-08-17	9.8	CVE-2026-74880
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a plugin sandbox bypass vulnerability where the PluginImportGuard blocks a different set of modules than the AST analyzer's DANGEROUS_MODULES set. Attackers can bypass AST analysis through string obfuscation or encoding to import unblocked dangerous modules like sys, shutil, multiprocessing, importlib, and pickle for arbitrary code execution.	2026-08-17	9.8	CVE-2026-74886
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 use HKDF with no salt and static info parameter in key normalization functions, reducing entropy extraction and determinism. Attackers can exploit predictable key derivation with identical inputs to weaken cryptographic security against multi-target attacks.	2026-08-17	9.8	CVE-2026-74889
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain hardcoded database credentials in standalone server configuration files. Attackers on the same network can access PostgreSQL databases using well-known default credentials to retrieve sensitive data.	2026-08-17	9.8	CVE-2026-74891
jahlikes--openssl_encrypt	openssl_encrypt before 1.4.0 contains an authentication bypass vulnerability in the verify_api_token function that accepts any non-empty Bearer token string without validation. Attackers can upload arbitrary public keys, enumerate all keys, and revoke keys belonging to any user by providing any Bearer token in the Authorization header.	2026-08-17	9.8	CVE-2026-74894
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 fail to apply sandbox restrictions in the default process isolation mode for plugin execution. Attackers can execute malicious plugins with unrestricted access to the filesystem, network, subprocess execution, and all Python modules.	2026-08-17	9.8	CVE-2026-74895
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a sandbox escape vulnerability in the DangerousPatternVisitor AST analyzer that fails to detect dunder attribute traversal techniques. Attackers can use __class__, __bases__, __subclasses__(), and __globals__ chains to access restricted functions and execute arbitrary system commands from plugin code.	2026-08-17	9.8	CVE-2026-74896
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a sandbox escape vulnerability in IsolatedPluginExecutor that exposes Python type objects in restricted exec() builtins. Attackers can traverse the Python class hierarchy via __class__.__mro__.__subclasses__() to access system functions and execute arbitrary OS commands.	2026-08-17	9.8	CVE-2026-74899
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a critical vulnerability in pqc.py where KEM decapsulation failures silently fall back to simulation mode, generating a deterministic shared secret from only 16 bytes of the private key and publicly available encapsulated key data. Attackers who obtain 16 bytes of the private key can compute the shared secret and decrypt all ciphertext, as the fallback triggers on any KEM failure without raising an error.	2026-08-17	9.8	CVE-2026-74900
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain an authentication bypass vulnerability in pqc.py where AES-GCM decryption failures trigger fallback to unauthenticated AES-CTR mode. Attackers can modify ciphertext in transit to bypass integrity verification and perform bit-flipping attacks without detection.	2026-08-17	9.8	CVE-2026-74901
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a missing ownership verification vulnerability in the revoke_key method that allows authenticated clients to revoke any other client's key. Attackers can revoke arbitrary keys by providing a valid ML-DSA signature, bypassing the intended ownership restriction.	2026-08-17	8.8	CVE-2026-74877

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a sandbox bypass vulnerability where the plugin sandbox fails to restrict alternative file access methods like pathlib.Path and io.open. Attackers can import pathlib or io modules to read and write arbitrary files, completely bypassing the restricted_open file access controls.	2026-08-17	8.8	CVE-2026-74883
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain hardcoded default JWT signing secrets in config.py that pass validation checks. Attackers with access to source code can forge valid JWT tokens for any client_id to gain authenticated access to keyserver and telemetry APIs.	2026-08-17	8.8	CVE-2026-74893
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 use Python's non-cryptographic random module for steganographic pixel selection in the generate_pseudorandom_sequence function. Attackers who know the password can recover the Mersenne Twister state from approximately 624 outputs and predict pixel locations containing hidden data for extraction.	2026-08-17	7.5	CVE-2026-74874
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain an information disclosure vulnerability in the /ready endpoint that returns full database exception strings to unauthenticated callers. Attackers can trigger database errors to extract sensitive information including hostnames, IP addresses, connection parameters, and potentially credentials from exception messages.	2026-08-17	7.5	CVE-2026-74879
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain an insecure default configuration that trusts the entire RFC 1918 private address space in IntegrityProxyConfig trusted_proxies. Attackers on private networks can forge client certificate headers to bypass mTLS authentication when ProxyAuth validation is relaxed or modified.	2026-08-17	7.5	CVE-2026-74882
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a path traversal vulnerability in the _is_safe_path method where the plugin_id parameter is not sanitized before constructing the plugin config directory path. Attackers can declare a malicious plugin_id containing path traversal sequences like '../' to access arbitrary directories outside the intended plugin directory.	2026-08-17	7.5	CVE-2026-74884
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 use a non-standard PBKDF2 key derivation construction with iterations=1 per call in an outer loop, creating a KDF whose security properties have not been formally analyzed. Attackers can exploit this weakened key derivation to more efficiently crack passwords protecting legacy encrypted files compared to standard PBKDF2 implementations.	2026-08-17	7.5	CVE-2026-74888
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a hardcoded default secret key in the standalone telemetry server configuration that is used for API key hashing. Attackers who know this default value can predict or forge API key hashes to compromise telemetry API authentication.	2026-08-17	7.5	CVE-2026-74892
jeecgboot--jimureport	JimuReport contains an authentication bypass vulnerability in the report folder template listing endpoint that allows unauthenticated attackers to enumerate all reports and retrieve share tokens. Attackers can use disclosed share tokens to access protected report endpoints and retrieve full report definitions including embedded SQL statements and live query data.	2026-08-17	7.5	CVE-2026-75479
jeemok--better-npm-audit	better-npm-audit through 3.11.0, and the 4.0.0-rc.2 prerelease, builds its npm audit command by interpolating the user-supplied --registry option into a command string in src/handlers/handleInput.ts without validation or quoting, then passes that string to child_process.exec() in index.ts, which spawns a shell. A registry value containing shell metacharacters such as a semicolon, pipe, or command substitution executes arbitrary operating system commands with the privileges of the process running the audit.	2026-08-22	7.8	CVE-2026-57998
Jeff Starr--BBQ Pro	Unauthenticated Cross Site Scripting (XSS) in BBQ Pro <= 3.9 versions.	2026-08-19	7.1	CVE-2026-73182
Jet Admin--Jet Admin	Jet Admin allows an attacker to create a malicious app and connect it to a target user's custom domain, edit the authentication configuration, and reroute traffic to the attacker-controlled app. Once connected to the target domain, the attacker's workspace is populated with the victim's OAuth Client ID and Client Secret if the victim is using an OAuth provider.	2026-08-21	8.6	CVE-2026-75932
Jet Admin--Jet Admin	Jet Admin allows an authenticated attacker to inject JavaScript via the sign-in page's scripts and styles option. Injected script is executed in the context of any visiting user's domain.	2026-08-21	7.3	CVE-2026-75933
JetBrains--IntelliJ IDEA	In JetBrains IntelliJ IDEA before 2026.2.1 rCE via Markdown export tool was possible	2026-08-17	7.8	CVE-2026-75056
JetBrains--PyCharm	In JetBrains PyCharm before 2026.2.1 code execution was possible via unauthenticated Jupyter MCP tools	2026-08-17	8.4	CVE-2026-75060
JetBrains--YouTrack	In JetBrains YouTrack before 2025.3.156085, 2026.1.13913, 2026.2.18112 an unauthenticated attacker could download database backups via shared draft signature	2026-08-17	9.1	CVE-2026-75045

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
JetBrains--YouTrack	In JetBrains YouTrack before 2025.3.156085, 2026.1.13914, 2026.2.18095 missing authorisation allowed an authenticated user to delete arbitrary entities via the mailbox endpoint	2026-08-17	8.1	CVE-2026-75044
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.18068 stored XSS via the fenced code-block language label was possible	2026-08-17	8.2	CVE-2026-75048
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.17917 unauthorised project transfer between organisations was possible	2026-08-17	8.1	CVE-2026-75051
JetBrains--YouTrack	In JetBrains YouTrack before 2026.1.13901, 2026.2.17950 doS attack was possible via crafted type parameters	2026-08-17	7.1	CVE-2026-75050
jetmonsters--Restaurant Menu by MotoPress	Unauthenticated Local File Inclusion in Restaurant Menu by MotoPress <= 2.4.11 versions.	2026-08-18	8.1	CVE-2026-73400
jhy--soup	jsoup through 1.23.2, fixed in commit 862ba2f, contains an uncontrolled resource consumption vulnerability in XmlTreeBuilder that allows remote attackers to exhaust JVM heap memory by supplying a deeply nested XML document with uniquely-namespaced elements. The builder copies the entire inherited namespace map on every start element, causing quadratic time and memory complexity, which attackers can exploit to trigger an OutOfMemoryError and terminate the application.	2026-08-20	7.5	CVE-2026-75140
jknack--handlebars.java	Handlebars.java provides logic-less and semantic Mustache templates with Java. Prior to 4.5.3, com.github.jknack.handlebars.springmvc.SpringTemplateLoader resolves attacker-influenced Spring MVC view names through Spring ResourceLoader without the path-containment validation used by other URL-based loaders. In handlebars-springmvc/src/main/java/com/github/jknack/handlebars/springmvc/SpringTemplateLoader.java, a view name using a file: or classpath: URL and ending with the # fragment delimiter places the appended .hbs suffix in the fragment, which FileUrlResource.exists() and URL.openStream() discard. HandlebarsViewResolver in handlebars-springmvc/src/main/java/com/github/jknack/handlebars/springmvc/HandlebarsViewResolver.java then passes the attacker-controlled name to handlebars.compile(), allowing an unauthenticated remote attacker to read files accessible to the JVM when an application exposes a controller with a user-influenced view name. This issue is fixed in version 4.5.3.	2026-08-20	7.5	CVE-2026-63490
Jonathan Daggerhart--Query Wrangler	Subscriber Remote Code Execution (RCE) in Query Wrangler <= 1.5.57 versions.	2026-08-20	9.9	CVE-2026-73992
KaizenCoders--URL Shortify	Unauthenticated Cross Site Scripting (XSS) in URL Shortify <= 2.5.0 versions.	2026-08-18	7.1	CVE-2026-73362
Kamlesh Parmar--Sync Post With Other Site	Contributor Arbitrary File Upload in Sync Post With Other Site <= 1.9.3 versions.	2026-08-18	9.9	CVE-2026-32463
kepano--defuddle	Defuddle cleans up HTML pages. Prior to 0.19.1, site extractors interpolate page-derived image alt and src values, og:image values, and video descriptions into HTML strings without context-appropriate escaping, and buildExtractorResponse() returns this contentHtml without the main pipeline's DOM-based sanitization. The affected paths include src/extractors/x-article.ts, src/extractors/substack.ts, and src/extractors/youtube.ts. A malicious page or attacker-controlled content on a matching domain can inject event-handler attributes or javascript URLs that execute when a victim or downstream application renders the extracted HTML. This issue is fixed in version 0.19.1.	2026-08-21	8.2	CVE-2026-61824
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 1.3.24, Kestra's custom Markdown parser in ui/src/utills/markdown_plugins/link.ts allows a user with permission to create or update a Flow description to inject JavaScript event-handler attributes through the custom [[link]] syntax, causing stored cross-site scripting when another user opens the description or information panel in the Flow list. This issue is fixed in version 1.3.24.	2026-08-18	8.7	CVE-2026-55839
keystonejs--keystone	Keystone is a content management system for Node.js. Prior to 6.5.3, the findMany resolver in packages/core/src/lib/core/queries/resolvers.ts compares the signed take argument directly with graphql.maxTake, allowing a remote unauthenticated GraphQL client to provide a negative take value whose magnitude exceeds the configured bound. The bypass also applies to relationship queries and can return more records than the developer intended, potentially exhausting service resources. This issue is fixed in version 6.5.3.	2026-08-21	7.5	CVE-2026-63421

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Kingtech LLC.--B2BKing Premium	Unauthenticated Cross Site Scripting (XSS) in B2BKing Premium <= 5.6.07 versions.	2026-08-20	7.1	CVE-2026-66598
KlbTheme--Total Donations	Unauthenticated Privilege Escalation in Total Donations <= 2.0.5 versions.	2026-08-19	9.8	CVE-2026-73390
KlbTheme--Total Donations	Unauthenticated SQL Injection in Total Donations <= 2.0.5 versions.	2026-08-19	9.3	CVE-2026-73391
koel--koel	Koel is a free, open-source music streaming solution. Prior to 9.7.1, outbound podcast and radio fetch paths perform a point-in-time App\Helpers\Network::isPublicHost() or isSafeUrl() check without pinning the validated address, and most paths lack redirect-hop validation and do not revalidate every redirect target. PhanAn\Poddle\Poddle::fromUrl(), PodcastService::getStreamableUrl(), PodcastService::isPodcastObsolete(), App\Rules\HasAudioContentType, and App\Rules\SafeUrl can therefore follow an attacker-controlled redirect to an internal address or connect after DNS rebinding changes a public resolution to a private one. These paths are reachable through podcast and radio APIs, including createPodcastChannel, createInternetRadioStation, refreshPodcasts, apiResource podcasts, and radio/stations, allowing an authenticated user to request internal services or cloud metadata and potentially receive parsed or streamed response content. This issue is fixed in version 9.7.1.	2026-08-19	7.1	CVE-2026-54491
koel--koel	Koel is a free, open-source music streaming solution. Prior to 9.7.0, the Subsonic-compatible createInternetRadioStation.view and updateInternetRadioStation.view routes accept an authenticated user's streamUrl without the SafeUrl and HasAudioContentType checks used by the regular radio API. app/Http/Requests/Subsonic/CreateInternetRadioStationRequest.php and app/Http/Requests/Subsonic/UpdateInternetRadioStationRequest.php pass the stored URL through app/Services/RadioService.php to app/Services/Radio/RadioStreamProxy.php, where RadioStreamProxy::openStream() calls fopen(\$url, 'r', false, \$context). Streaming /radio/stream/{id} returns the upstream response body, allowing access to loopback, RFC1918, Docker bridge, metadata, or other internal HTTP services reachable from the Koel server. This issue is fixed in version 9.7.0.	2026-08-19	7.7	CVE-2026-54493
Kovah--LinkAce	LinkAce is a self-hosted archive to collect website links. Prior to version 2.5.7, the Bulk Link API endpoint ('POST /api/v2/bulk/links') accepts URLs without any format validation, allowing an authenticated user to store a 'javascript:' URI. The stored URI is later rendered verbatim as an 'href' in Blade templates, and clicking it executes arbitrary JavaScript in the victim's browser - exfiltrating cookies and session tokens. Version 2.5.7 fixes the issue.	2026-08-20	7.3	CVE-2026-49436
LabRedesCefetRJ--WeGIA	WeGIA before 3.9.2 contains an authorization bypass vulnerability in the password change flow that allows any authenticated user to change their account password without providing existing credentials by exploiting the unconditional exclusion of the alterarSenha method from permission checks in controle/control.php. Attackers can manipulate the redir parameter to point to alterar_senha.php, routing through verificarSenhaConfig() instead of verificarSenha() to bypass current password verification and convert temporary session access into permanent account takeover.	2026-08-20	8.1	CVE-2026-76633
langbot-app--LangBot	LangBot is a global IM bot platform designed for LLMs. In version 4.10.7 and earlier, any authenticated user can add or change an STDIO MCP server configuration without an adequate authorization boundary. In src/langbot/pkg/provider/tools/loaders/mcp.py, StdioServerParameters accepts the configured command and arguments and starts a server-side subprocess on the LangBot server. An attacker who can sign up or obtain an account can use the Extensions MCP configuration to execute arbitrary commands with the privileges of the LangBot service, enabling data disclosure, modification, and service disruption. No fixed version is available as of this review.	2026-08-20	8.8	CVE-2026-54449
langchain-ai--langchain-community	SitemapLoader.parse_sitemap in langchain_community/document_loaders/sitemap.py applies the documented restrict_to_same_domain control only to leaf url entries. The loop over url elements filters cross-domain locations, but the loop over nested sitemap elements passes the child loc straight to self.scrape_all([loc.text], "xml"), which reaches WebBaseLoader.scrape_all and an aiohttp GET, with no domain comparison and no check for private, loopback or link-local destinations. An attacker who controls or influences an ingested sitemap can therefore point a nested sitemap entry at an internal address and make the server fetch it even	2026-08-20	8.6	CVE-2026-72848

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	when the deploying application set restrict_to_same_domain to True specifically to confine outbound requests. The fetched content is parsed and surfaces in the returned Documents, so internal responses are disclosed to the caller rather than merely requested.			
LCweb--Global Gallery	Unauthenticated Cross Site Scripting (XSS) in Global Gallery <= 11.1.2 versions.	2026-08-19	7.1	CVE-2026-73184
Legora--Legora	Legora before 2026-08-14 contains a cross-site scripting vulnerability that allows attackers to achieve arbitrary JavaScript execution in a victim's browser by embedding a Mermaid block prefixed with a gray-matter JavaScript front-matter directive, causing the front-matter parser to invoke eval() before any SVG sanitization occurs. Attackers can exploit this flaw through influenced Mermaid diagram content to execute arbitrary JavaScript in the user's browser context, with elevated impact on Word and Outlook add-in surfaces where bearer session tokens are persisted in localStorage.	2026-08-17	7.7	CVE-2026-74234
libevent--libevent	Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent has a heap out-of-bounds write in bufferevent_sock.c when bufferevent_socket_set_conn_address_ copies a kernel-supplied AF_UNIX peer address into bufferevent_private.conn_address. Release builds compiled with NDEBUG disable the EVUTIL_ASSERT length guard, and the evhttp accept path can pass a 110-byte sockaddr from accept() into the 28-byte field. An unauthenticated local peer able to connect to an AF_UNIX listener can overwrite the adjacent dns_request pointer and heap data, causing memory corruption with confidentiality, integrity, and availability impact. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.	2026-08-20	8.4	CVE-2026-63388
libevent--libevent	Libevent is an event notification library. Prior to 2.1.13 and 2.2.2-alpha, libevent has an off-by-one stack buffer overflow in evdns.c when dnsname_to_labels formats a name-bearing DNS record at the end of the 64 KB stack buffer allocated by evdns_server_request_format_response. The final-label check permits j plus label_len plus one to equal buf_len, after which the terminating null byte is written to buf[buf_len]. A crafted DNS server response containing PTR, CNAME, MX, NS, or SOA data can trigger the one-byte out-of-bounds write and crash or corrupt the process. This issue is fixed in versions 2.1.13 and 2.2.2-alpha.	2026-08-20	7	CVE-2026-63387
libevent--libevent	Libevent is an event notification library. From 2.2.0-alpha-dev until 2.2.2-alpha, the libevent WebSocket server in ws.c accumulates fragmented frames in evws->incomplete_frames without enforcing a total message-size limit. An unauthenticated remote client can repeatedly send fragmented WebSocket frames below WS_MAX_RECV_FRAME_SZ with FIN=0, causing the evbuffer to grow without bound until the process or host exhausts memory. This issue is fixed in version 2.2.2-alpha.	2026-08-20	7.5	CVE-2026-63495
libexpat project--libexpat	Expat through 2.8.3 contains a denial of service vulnerability caused by quadratic algorithmic complexity in the storeAtts() function in xmlparse.c, where processing N specified attributes with non-normalized values triggers an O(N^2) linear scan of elementType->defaultAtts to determine CDATA status. A remote unauthenticated attacker can supply a single well-formed XML document of a few megabytes to an application parsing untrusted XML to cause excessive CPU consumption, resulting in denial of service without requiring authentication, external entity resolution, or non-default parser options.	2026-08-18	7.5	CVE-2026-66046
libexpat--libexpat	Expat through 2.8.3 contains an out-of-bounds read vulnerability that allows attackers to trigger memory corruption by processing XML with external entity parsers created via XML_ExternalEntityParserCreate. A struct size mismatch between ELEMENT_TYPE members causes storeAtts to read the attIndex member past allocated memory boundaries, resulting in failure to normalize whitespace in non-CDATA attributes or a wild pointer dereference causing a segfault. This vulnerability was introduced by the fix for CVE-2026-66046.	2026-08-20	7.5	CVE-2026-76641
libfuse--sshfs	SSHFS is a network filesystem client for connecting to SSH servers. Prior to version 3.7.6, a rogue SFTP server can return absolute symlink targets or relative targets containing parent-directory components that SSHFS passes through FUSE for resolution by the client kernel against the local filesystem. The documented transform_symlinks mitigation does not contain relative targets because transform_symlink() returns early at sshfs.c:2181, while sshfs_readlink() at sshfs.c:2234 to sshfs.c:2236 otherwise copies the server-supplied link target to the kernel. A victim or victim-side tool that follows such a link through ordinary operations such as cp, rsync, backup tooling, or an editor can disclose readable local files back to the server or write server-controlled content to writable local	2026-08-19	9.3	CVE-2026-47187

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	files, potentially including startup or scheduled-task files. This issue is fixed in version 3.7.6.			
libfuse--sshfs	SSHFS is a network filesystem client for connecting to SSH servers. From version 1.4 until 3.7.6, SSHFS accepts a bracketed mount source such as [-oProxyCommand=CMD]:/path and find_base_path() removes the brackets, leaving a host value that begins with - and is passed directly to ssh as a command-line argument. When a caller also supplies a path-valued sftp_server, ssh treats the normalized host as an option and the server path as its destination, causing an injected ProxyCommand to execute locally before any connection or authentication succeeds. The attack requires a caller or wrapper that passes an attacker-controlled mount source to SSHFS with the required sftp_server configuration and results in arbitrary command execution as the user running SSHFS. This issue is fixed in version 3.7.6.	2026-08-19	7	CVE-2026-48711
libgit2--libgit2	libgit2 is a portable C implementation of the Git core methods provided as a linkable library with a solid API, allowing to build Git functionality into your application. Prior to 1.8.6 and 1.9.5, libgit2 performs a fixed-size strncmp in set_data in src/libgit2/transport/smart_pkt.c without first verifying that the smart-protocol pkt-line capability buffer contains 14 bytes. A malicious Git server can make bytes after the pkt-line complete object-format=, causing format_str to advance beyond the pkt-line and the following memchr length calculation to underflow. The resulting heap out-of-bounds walk can crash a client during the first refs-advertisement packet over HTTP, HTTPS, SSH, or the Git protocol. This issue is fixed in versions 1.8.6 and 1.9.5.	2026-08-20	7.5	CVE-2026-53587
LibVNC--libvncserver	LibVNClient is a library for easy implementation of a VNC client. In versions 0.9.12 through 0.9.15, a malicious (or man-in-the-middle) VNC server can force a connecting 'libvncclient' to write attacker-controlled data past the end of its framebuffer. This is an out-of-bounds heap write with attacker-controlled length, contents, and offset. It needs no authentication (the attacker is the server), works in a default build with default settings, and fires from a single 'FramebufferUpdate' the moment the victim connects. It crashes any client unconditionally (denial of service); we also demonstrated it overwriting an application callback pointer and redirecting execution to attacker-chosen code (code execution) under the default configuration. Commit 540332be3e0acc566fa64da6f1b4680c72c724dd patches the issue.	2026-08-21	8.8	CVE-2026-50538
liedekef--Events Made Easy	The Events Made Easy plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.2.5 via the eme_single_event_page_template function. This makes it possible for authenticated attackers, with contributor-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included. The stored traversal payload is triggered passively when any visitor loads the affected single-event page, meaning post-submission execution does not require additional attacker interaction.	2026-08-20	7.5	CVE-2026-75963
liftoff-sr--CIPster	A security flaw has been discovered in liftoff-sr CIPster 1802525be27d33e19a9a83c163e331a1d13b1892. The impacted element is the function CipAttribute::GetAttrData/CipAttribute::SetAttrData of the file ciptypes.h of the component Generic Attribute Logic. Performing a manipulation results in memory corruption. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The patch is named e745d9d4a8ca3a13689066983a1269fe1e567674. It is suggested to install a patch to address this issue.	2026-08-20	7.3	CVE-2026-76987
Linuxfabrik--monitoring-plugins	linuxfabrik-lib provides Python modules for database access, caching, shell execution, and API integrations, and Linuxfabrik Monitoring Plugins uses those modules to run external monitoring commands. From the earliest affected releases until linuxfabrik-lib 5.0.0 and Linuxfabrik Monitoring Plugins 6.0.0, check plugins embedded user-controlled values in command strings passed to lib.shell.shell_exec(), which split strings at pipe characters and executed the resulting commands. In check-plugins/restic-check/restic-check, the --repo parameter could inject a pipe-delimited command into a constructed restic invocation, and sudo-authorized execution allowed a compromised nagios or icinga account to run that command as root. The shared library also accepted command strings and a shell parameter, while numerous plugins constructed external commands from attacker-influenced arguments. The fixes require argv lists, always use shell=False, remove pipe splitting, and reject option-like positional values	2026-08-18	7.8	CVE-2026-55426

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	through lib.shell.safe_cli_value(). These issues are fixed in linuxfabrik-lib 5.0.0 and Linuxfabrik Monitoring Plugins 6.0.0.			
logto-io--logto	Logto is the modern, open-source auth infrastructure for SaaS and AI apps. Prior to 1.41.0, Logto's email subaddressing blocklist in packages/core/src/libraries/sign-in-experience/email-blocklist-policy.ts used the attacker-controlled domain from email input to construct subaddressingRegex when blockSubaddressing was enabled. The permissive emailRegExp accepted multiple at signs and regular expression metacharacters, and POST /api/experience/verification/verification-code could therefore cause catastrophic backtracking in subaddressingRegex.test(email). The resulting event-loop stall could make authentication, token issuance, SSO, and the administrative console unavailable. This issue is fixed in version 1.41.0.	2026-08-19	7.5	CVE-2026-62317
louislam--dockge	Dockge validates a stack name only on the write path. In backend/stack.ts the allow-list check in validate(), which requires the name to match ^[a-z0-9_-]+\$ is reached from save() alone, while the path getter returns path.join(this.server.stacksDir, this.name) and Stack.getStack builds path.join(server.stacksDir, stackName) with no check. The socket handlers in backend/agent-socket-handlers/docker-socket-handler.ts confirm the caller is logged in and that the name is a string, then pass it straight to Stack.getStack, so a name containing traversal sequences resolves outside the managed stacks directory. An authenticated user can therefore read the composeENV and composeYAML values of any directory the server process can reach, which discloses the secrets in that directory's .env or Compose file, and can invoke delete(), which runs docker compose down and then fsAsync.rm on the traversed path with recursive and force set, removing that directory. Disclosure is limited to files named .env or an accepted Compose filename, and deletion requires the target directory to hold a valid Compose file so that docker compose down exits successfully. Dockge commonly runs as root with access to the Docker socket, so the reachable set includes unrelated applications on the host. Instances configured with disableAuth, a supported option that logs the caller in as admin automatically, expose both operations without authentication.	2026-08-20	8.8	CVE-2026-73040
lukeseager--WordPress Persistent Login	Subscriber SQL Injection in WordPress Persistent Login <= 3.1.0 versions.	2026-08-20	8.5	CVE-2026-66594
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.2.0, a specially crafted image can be used to read or create/write arbitrary files on the host; possibly leading to arbitrary command execution. Version 7.2.0 fixes the issue.	2026-08-21	9.9	CVE-2026-48749
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.2.0, the 'record-output' parameter of the '/instances/\$name/exec' endpoint stores the output of the command in the 'exec-output' directory of the instance. If 'exec-output' is a symlink, file named 'exec_UUID.stdout' and 'exec_UUID.stderr' can be written to an arbitrary location where the '.stdout' file will contain arbitrary content. This behavior can be abused for arbitrary command execution. Version 7.2.0 contains a patch.	2026-08-21	9.9	CVE-2026-48750
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.2.0, instance snapshots ignore the 'restricted.containers.lowlevel=block' setting; allowing for arbitrary command execution on the Incus server by abusing lowlevel hooks such as 'raw.lxc' and 'raw.qemu'. Version 7.2.0 patches the issue.	2026-08-21	9.9	CVE-2026-48751
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.2.0, a specially crafted image or instance backup can be used to read or create/write arbitrary files on the host; possibly leading to arbitrary command execution. Version 7.2.0 patches the issue.	2026-08-21	9.9	CVE-2026-48752
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.1.0, the S3 protocol upload endpoint is vulnerable to path traversal and allows creation of arbitrary files on the host. This behavior could lead to arbitrary command execution. Version 7.1.0 fixes the issue.	2026-08-21	9.9	CVE-2026-48753
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.1.0, improper validation of user-provided backup compression algorithm leads to argument injection in the constructed command line. This leads to an arbitrary file write on the host, possibly leading to arbitrary command execution. Version 7.1.0 patches the issue.	2026-08-21	9.9	CVE-2026-48755
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.2.0, an arbitrary file write exists in the Incus client when a malicious image server returns a	2026-08-21	9.9	CVE-2026-48769

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	crafted `Incus-Image-Hash` header. This can lead to arbitrary command execution as root on the server. Version 7.2.0 patches the issue.			
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.3.0, improper validation of user-provided `block.create_options` in storage volume configuration leads to argument injection in the constructed filesystem creation command line. This allows a project-scoped user to inject arbitrary arguments into the binary executed as root. Version 7.3.0 patches the issue.	2026-08-21	9.9	CVE-2026-62867
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.3.0, when migrating an instance to another cluster member, user-supplied configuration overrides (including security-critical keys like `security.privileged` and `raw.lxc`) are applied without any project restriction enforcement, allowing a restricted project user to escalate to a privileged container and escape to the host. Version 7.3.0 patches the issue.	2026-08-21	9.9	CVE-2026-62940
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.3.0, when copying an instance across projects, the project restriction check (`AllowInstanceCreation`) runs BEFORE the source instance's configuration is merged into the request. Dangerous configuration keys (including `security.privileged`, `raw.lxc`, `raw.apparmor`) from the source instance are merged AFTER the check passes, bypassing all project restrictions on the target project. Version 7.3.0 patches the issue.	2026-08-21	9.9	CVE-2026-62941
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.3.0, an unprivileged, project-confined Incus user (a non-admin TLS/RBAC identity with `can_create_images` and `can_create_instances`) can execute arbitrary code as root on the host. A crafted image ships `backup.yaml` as a symlink to a host file. When the root daemon writes the instance's backup file, it follows the symlink. Version 7.3.0 patches the issue.	2026-08-21	9.9	CVE-2026-63125
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.3.0, a malicious image containing a `metadata.yaml` symlink pointing to an arbitrary host path allows an authenticated Incus user to read or overwrite any file on the host as root via the instance metadata API. The `exec-output` and `templates/` paths were patched in a prior release using `Lstat` rejection and `os.OpenRoot` confinement; `metadata.yaml` was not included in either patch and remains exploitable. Version 7.3.0 patches the issue.	2026-08-21	9.9	CVE-2026-63343
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.2.0, missing authorization checks exist for custom volume copying where an attacker knowing the name of a project that they don't have access to and the name of a custom volume in that project can copy the custom volume to a new project. This issue could allow an attacker to access secrets in custom volumes they are not authorized to access. Version 7.2.0 patches the issue.	2026-08-21	7.7	CVE-2026-55621
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.2.0, missing authorization checks exist for instance copying where an attacker knowing the name of a project that they don't have access to and the name of an instance in that project can copy the instance to a new project. This issue could allow an attacker to access secrets in instances they are not authorized to access. Version 7.2.0 patches the issue.	2026-08-21	7.7	CVE-2026-55622
lxml--lxml	lxml is a library for processing XML and HTML in the Python language. Prior to 6.1.1, link attributes in ``lxml.html.defs.link_attrs`` were missing ``xlink:href``, which can be used for URL bypass attacks in embedded SVG/MathML/etc. content. This vulnerability was fixed in lxml 6.1.1 and lxml_html_clean 0.4.5.	2026-08-20	8.2	CVE-2026-49825
lxml--lxml	Seroyal facilitates JS value stringification, including complex structures beyond JSON.stringify capabilities. Prior to 1.5.3, seroyal.fromJSON() allows attacker-controlled JSON Promise control nodes to operate on values from the general deserialization reference table without verifying genuine internal Promise resolver records, causing deserialization side effects with plugins enabled and potentially unintended server-side invocation or remote code execution when downstream frameworks register callable wrappers. This issue is fixed in version 1.5.3.	2026-08-18	9.8	CVE-2026-59940
M2Team--NanaZip	NanaZip is the 7-Zip derivative intended for the modern Windows experience. From version 1.0.88.0 until stable version 6.0.1698.0 and preview version 6.5.1742.0, the Lz4Decode function in NanaZip.Core/SevenZip/CPP/7zip/Archive/SquashfsHandler.cpp rejects only a zero return from LZ4_decompress_safe even though malformed input produces a negative error value. The negative int is converted to the unsigned SizeT destLen and then truncated into outBufWasWrittenSize, causing ReadBlock to trust an attacker-inflated cachedUnpackBlockSize. During fragment extraction, an	2026-08-20	7.1	CVE-2026-54616

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker-controlled inode Offset can make memcpy read beyond the _cachedBlock heap allocation and place adjacent heap contents in the extracted file, or crash the process. This issue is fixed in stable version 6.0.1698.0 and preview version 6.5.1742.0.			
maartenbelmans--Advanced Product Fields (Product Addons) for WooCommerce	The Advanced Product Fields (Product Addons) for WooCommerce plugin for WordPress is vulnerable to Improper Input Validation in all versions up to, and including, 1.6.21. This is due to a logic flaw in the 'validate_cart_data' function. This makes it possible for unauthenticated attackers to bypass required paid addons and complete purchases at the base product price only, effectively stealing products by paying a fraction of the intended total. The vulnerability was partially patched in version 1.6.19.	2026-08-22	7.5	CVE-2026-2996
Magazine3--WP Multilang	Unauthenticated Cross Site Scripting (XSS) in WP Multilang <= 2.4.31 versions.	2026-08-18	7.1	CVE-2026-73342
mailgun--Mailgun for WordPress	The Mailgun for WordPress plugin for WordPress is vulnerable to Server-Side Request Forgery (SSRF) via path traversal in versions up to and including 2.2.0. This is due to insufficient input validation in the add_list() function, which accepts user-controlled array keys from \$_POST['addresses'], passes them through sanitize_text_field(). This makes it possible for unauthenticated attackers to make authenticated POST requests to any Mailgun API endpoint using the WordPress site's API key, including creating inbound email-forwarding routes that can intercept password reset emails, leading to administrator account takeover.	2026-08-22	9.8	CVE-2026-78003
Mailu--Mailu	Mailu is a mail server as a set of Docker images. Prior to version 2024.06.52, a missing authorization check in the Mailu admin REST API allows any unauthenticated attacker to remove any potential IP restriction or update the comment field from any existing user token provided the REST API is enabled. Upgrade to Mailu 2024.06.52 to receive a patch or, as a workaround, turn the REST API off.	2026-08-20	7.5	CVE-2026-49217
MakeWebBetter--MWB HubSpot for WooCommerce	Subscriber Broken Authentication in MWB HubSpot for WooCommerce <= 1.6.7 versions.	2026-08-18	7.1	CVE-2026-73396
marc4--Security Hardener	The Security Hardener plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 2.4.4. The vulnerability exists because the plugin's user-enumeration protection, which is enabled by default, hooks the rest_endpoints filter via secure_user_endpoints() and overwrites every registered handler's permission_callback on both the /wp/v2/users and /wp/v2/users/(?P<id>[\d]+) routes - including POST, PUT, PATCH, and DELETE handlers - with a bare closure that returns only is_user_logged_in(), completely stripping WordPress Core's original capability checks such as create_users, promote_user, edit_users, and delete_users that WP_REST_Users_Controller normally enforces. This makes it possible for authenticated attackers with Subscriber-level access and above to create new Administrator accounts by sending POST request to /wp/v2/users with administrator role, or to reset an existing Administrator's password by issuing a PUT/POST request to /wp/v2/users/<id>. Because the block_user_enum option defaults to enabled, no special plugin configuration is required - the overwrite is active on every request as soon as the plugin is installed.	2026-08-22	8.8	CVE-2026-16149
marimo-team--marimo	marimo before 0.23.15 contains a code injection vulnerability in the notebook configuration handler that allows attackers to execute arbitrary commands by supplying a crafted MCP server entry with an attacker-controlled command value embedded in a notebook. When the notebook is opened in edit mode, marimo launches the specified command as a local subprocess before any notebook cell is executed, requiring no authentication or cell execution to trigger the vulnerability.	2026-08-19	8.8	CVE-2026-75149
masteriyo--Masteriyo - LMS	Unauthenticated Arbitrary File Upload in Masteriyo - LMS <= 2.3.2 versions.	2026-08-18	9.8	CVE-2026-73996
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. Prior to 4.4.19 and from 4.5.0 until 4.5.12, Mastodon's app/models/concerns/user/ldap_authenticable.rb mutates OpenSSL::SSL::SSLContext::DEFAULT_PARAMS when LDAP authentication uses LDAP_TLS_NO_VERIFY=true, disabling SSL and TLS certificate verification globally for requests made by puma web processes while sidekiq background jobs remain unaffected. This issue is fixed in versions 4.4.19 and 4.5.12.	2026-08-18	7.4	CVE-2026-59825
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.6, 10.11.x <= 10.11.21, 11.8.x <= 11.8.3 fail to validate BoardMember.Scheme* fields server-side on insert and archive-import paths which allows a board editor or non-guest team member to grant board	2026-08-17	8.3	CVE-2026-9816

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	admin to arbitrary users via POST /api/v2/boards/{boardID}/members and POST /api/v2/teams/{teamID}/archive/import.. Mattermost Advisory ID: MMSA-2026-00685			
max-mapper--extract-zip	extract-zip through 2.0.1 containment-checks only the parent directory of each archive entry and never the entry's own final path component, so an archive containing two entries with identical names - a symlink whose target is outside the destination, followed by a regular file - writes through the planted symlink and yields an arbitrary file write outside the destination directory.	2026-08-17	8.1	CVE-2026-19693
mdmag--Quill Forms Conversational Multi Step Forms, Surveys & quizzes	The Quill Forms Conversational Multi Step Forms, Surveys & quizzes plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.7.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-18	7.2	CVE-2026-75091
Melograno Venture Studio--wpDataTables	Unauthenticated Cross Site Scripting (XSS) in wpDataTables <= 6.5.1.4 versions.	2026-08-20	7.1	CVE-2026-66597
MemTensor--MemOS	MemOS is a memory operating system for LLMs and AI agents. In deployments where authentication is enabled (AUTH_ENABLED=true) but the undocumented, defaultless INTERNAL_SERVICE_SECRET environment variable is unset, the is_internal_request() check in src/memos/api/middleware/auth.py fails open: os.getenv("INTERNAL_SERVICE_SECRET") returns None and a request omitting the X-Internal-Service header also yields None, so the comparison None == None evaluates true. The request is then treated as a trusted internal principal and granted scopes: ["all"]. As a result, an unauthenticated remote attacker can reach the admin API-key management endpoints to mint API keys for any user, enumerate keys, revoke keys, and generate a master key for persistent privileged access, as well as all data endpoints.	2026-08-17	9.8	CVE-2026-75110
merkulove--Readabler	Unauthenticated SQL Injection in Readabler < 2.0.18 versions.	2026-08-18	9.3	CVE-2026-74015
Metagauss--RegistrationMagic	Unauthenticated PHP Object Injection in RegistrationMagic <= 6.0.9.7 versions.	2026-08-18	9.8	CVE-2026-73341
Microsoft--Azure ARC	Incorrect authorization in Azure Arc allows an unauthorized attacker to elevate privileges over a network.	2026-08-20	10	CVE-2026-69555
Microsoft--Azure Data Factory	Improper verification of cryptographic signature in Azure Data Factory allows an unauthorized attacker to elevate privileges over a network.	2026-08-20	9.3	CVE-2026-62834
Microsoft--Azure Data Factory	Server-side request forgery (ssrf) in Azure Data Factory allows an unauthorized attacker to disclose information over a network.	2026-08-20	8.6	CVE-2026-66800
Microsoft--Azure Data Manager for Energy	Integer overflow or wraparound in Azure Data Manager for Energy allows an authorized attacker to execute code over a network.	2026-08-20	8.5	CVE-2026-69419
Microsoft--Azure Logic Apps	Improper limitation of a pathname to a restricted directory ('path traversal') in Azure Logic Apps allows an unauthorized attacker to elevate privileges over a network.	2026-08-20	9.6	CVE-2026-69400
Microsoft--Azure Managed Instance for Apache Cassandra	Improper neutralization of argument delimiters in a command ('argument injection') in Azure Managed Instance for Apache Cassandra allows an unauthorized attacker to execute code over a network.	2026-08-20	10	CVE-2026-65770
Microsoft--Azure SQL Database	Server-side request forgery (ssrf) in Azure SQL Database allows an unauthorized attacker to elevate privileges over a network.	2026-08-21	10	CVE-2026-69502
Microsoft--Azure SQL Database	Improper access control in Azure SQL Database allows an authorized attacker to elevate privileges over a network.	2026-08-20	9.1	CVE-2026-66309
Microsoft--Azure SQL Database	Improper neutralization of special elements used in an sql command ('sql injection') in Azure SQL Database allows an authorized attacker to elevate privileges over a network.	2026-08-20	9.9	CVE-2026-68782
Microsoft--Azure SQL Database	Improper neutralization of special elements used in an sql command ('sql injection') in Azure SQL Database allows an authorized attacker to elevate privileges over a network.	2026-08-20	9.9	CVE-2026-68789
Microsoft--Azure Stack HCI	Observable response discrepancy in Azure Stack HCI allows an unauthorized attacker to disclose information over a network.	2026-08-20	8.6	CVE-2026-69519
Microsoft--Azure Virtual Machines	Server-side request forgery (ssrf) in Azure Virtual Machines allows an authorized attacker to elevate privileges over a network.	2026-08-20	8.5	CVE-2026-69543
Microsoft--Azure Web Apps	Use of incorrectly-resolved name or reference in Azure Arc allows an unauthorized attacker to elevate privileges over a network.	2026-08-20	10	CVE-2026-65816

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Copilot Web	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to disclose information over a network.	2026-08-18	8.8	CVE-2026-24301
Microsoft--Microsoft Copilot in Azure	Server-side request forgery (ssrf) in Microsoft Copilot in Azure allows an authorized attacker to disclose information over a network.	2026-08-20	7.7	CVE-2026-69855
Microsoft--Microsoft Entra	Deserialization of untrusted data in Microsoft Entra ID allows an unauthorized attacker to execute code over a network.	2026-08-20	10	CVE-2026-69836
Microsoft--Microsoft Entra	Server-side request forgery (ssrf) in Azure Active Directory allows an authorized attacker to elevate privileges over a network.	2026-08-20	9.9	CVE-2026-69851
Microsoft--Microsoft Exchange Online	Server-side request forgery (ssrf) in Microsoft Exchange Online allows an unauthorized attacker to elevate privileges over a network.	2026-08-20	10	CVE-2026-65801
Microsoft--Microsoft Fabric	Relative path traversal in Microsoft Fabric allows an authorized attacker to elevate privileges over a network.	2026-08-20	9.9	CVE-2026-63509
Microsoft--Microsoft Partner Center	Authorization bypass through user-controlled key in Microsoft Partner Center allows an unauthorized attacker to disclose information over a network.	2026-08-20	8.6	CVE-2026-69558
microsoft--UFO	Microsoft UFO open-source framework for intelligent automation across devices and platforms. Prior to 3.0.8, ufo/client/mcp/http_servers/linux_mcp_server.py binds a FastMCP streamable HTTP server to localhost:8010 but does not validate the Host, Origin, or Sec-Fetch-Site headers. An attacker-controlled web page can use DNS rebinding to reach the local /mcp endpoint, enumerate tool schemas through tools/list, and invoke execute_command with a valid UFO_MCP_API_KEY to read files or execute allowed operating system commands as the victim's user. This issue is fixed in version 3.0.8.	2026-08-21	8.8	CVE-2026-62316
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-08-19	7	CVE-2026-62727
Microsoft--Windows Remote Help	Uncontrolled search path element in Windows Remote Help Defense allows an authorized attacker to perform spoofing locally.	2026-08-20	7.1	CVE-2026-55013
miniOrange--WordPress Social Login and Register	Unauthenticated Cross Site Scripting (XSS) in WordPress Social Login and Register <= 7.8.1 versions.	2026-08-18	7.1	CVE-2026-73351
mlflow--mlflow	MLflow is an open source AI engineering platform for agents, large language models, and machine learning models. Prior to 3.15.0, the unauthenticated POST /api/2.0/mlflow/webhooks/{id}/test endpoint calls _validate_webhook_url() in mlflow/utlis/validation.py only for the original URL while mlflow/webhooks/delivery.py follows redirects and re-resolves the hostname without pinning the validated address, allowing attackers to reach internal or cloud metadata services and receive response_status and response_body. This issue is fixed in version 3.15.0.	2026-08-17	9.3	CVE-2026-64849
mlflow--mlflow	MLflow is an open source AI engineering platform for agents, large language models, and machine learning models. Prior to 3.15.0, CreateModelVersion accepts a run_id or model_id after _validate_source_run() or _validate_source_model() in mlflow/server/handlers.py verifies only path containment, allowing authenticated users to create a model version that references another user's artifact directory and read files through GET /model-versions/get-artifact without the required READ permission. This issue is fixed in version 3.15.0.	2026-08-17	7.1	CVE-2026-69148
Mohamed Magdy--Quill Forms	Unauthenticated Cross Site Scripting (XSS) in Quill Forms <= 5.7.1 versions.	2026-08-18	7.1	CVE-2026-28568
Monkeysan--Flatastic	Unauthenticated PHP Object Injection in Flatastic <= 2.0 versions.	2026-08-20	9.8	CVE-2026-66672
Monkeysan--Flatastic	Unauthenticated Cross Site Scripting (XSS) in Flatastic <= 2.0 versions.	2026-08-20	7.1	CVE-2026-66673
monkeytypegame--monkeytype	Monkeytype is a minimalistic and customizable typing test. In 26.26.0 and earlier, the backend rate-limit key generator in backend/src/middlewares/rate-limit.ts uses client-controlled cf-connecting-ip and x-forwarded-for headers before the trust-proxy-derived req.ip value. An unauthenticated attacker can rotate either header to create a new bucket for each request, bypassing rootRateLimiter, badAuthRateLimiter, getKey(), and the getKeyWithUid() fallback used by public endpoints. This permits repeated POST /users/forgotPasswordEmail and verificationEmail requests, mail bombing registered users, consuming Firebase or	2026-08-20	7.5	CVE-2026-69183

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SMTP quota, evading brute-force protection, and enabling resource exhaustion. Exploitability of cf-connecting-ip depends on deployment topology, but x-forwarded-for and direct-to-origin paths remain affected when those values are not overwritten by a trusted proxy. No fixed version is available as of this review.			
mybb--mybb	MyBB is free and open source forum software. From 1.8.13 until 1.8.40, the installer module does not properly escape user-supplied database configuration values written to the configuration file, resulting in PHP code injection and remote code execution when the installer is available. install/index.php processes the values with addslashes(), but the \$characters argument added in MyBB 1.8.13 does not include the backslash character, allowing crafted input to escape the generated PHP string. The uniquely identifying implementation details include introduced in MyBB 1.8.13. This issue is fixed in version 1.8.40.	2026-08-18	9.8	CVE-2026-45117
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the Contact module does not validate a redirect URL or protocol correctly, resulting in an open redirect and reflected JavaScript code injection. contact.php accepts the redirect target from the from HTTP parameter in \$mybb->input['from'] or the Referer HTTP header in \$_SERVER['HTTP_REFERER'] and passes it to redirect() without sufficient verification. A javascript: URI becomes the target of the 'Click here if you don't want to wait any longer' link because \$force_redirect is true, allowing script execution when a victim selects the link. This issue is fixed in version 1.8.40.	2026-08-18	9.3	CVE-2026-45118
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the Buddy/Ignore component does not sanitize usernames correctly, allowing attackers to perform JavaScript code injection through a specially crafted username. The User CP Buddy/Ignore list and the Select Buddies list in Private Messages pass usernames through htmlspecialchars_uni(), which may leave single quotes unescaped. The payload is triggered when a victim chooses Yes in Please Confirm while removing the username in usercp.php, or selects the username through the onclick handler in the xmlhttp.php Select Buddies popup. The uniquely identifying implementation details include Private Messages Select Buddies list, and unescaped single quotes. This issue is fixed in version 1.8.40.	2026-08-18	8.7	CVE-2026-45115
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the user datahandler does not properly validate checkbox and multiselect profile field types, resulting in stored JavaScript code injection. UserDataHandler::verify_profile_fields() only performs the specialized validation when is_array(\$profile_fields[\$field]) is true. A non-array profile_fields[fidX] value instead of the expected profile_fields[fidX][] shape falls through to generic text handling and is stored without verification. The affected value is then rendered directly by member.php and inc/functions_post.php rather than processed by the MyCode parser. The uniquely identifying implementation details include inc/datahandlers/user.php. This issue is fixed in version 1.8.40.	2026-08-18	8.7	CVE-2026-45116
Netatalk--netatalk	Netatalk is a Free and Open Source file server suite for Unix-like operating systems. In versions 3.1.19 through 4.4.2, a stack-based buffer overflow exists in the deletedir() function of Netatalk's afpd daemon due to an integer underflow in the calculation of the remaining buffer size used for path construction. deletedir() is a utility function called when a file operation crosses a device boundary inside an AFP shared volume, which the standard library's renameat() cannot handle. The function attempts to prevent buffer overflows by tracking available space in a size_t remain variable. However, the arithmetic used to compute remain results in an unsigned integer underflow, causing the variable to become SIZE_MAX. Because of this, the subsequent boundary check always evaluates as safe, allowing an unbounded strcpy() operation to copy attacker-controlled filenames into a nearly full stack buffer. Version 4.4.3 patches the issue.	2026-08-17	7.5	CVE-2026-45698
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.2, authenticated users could influence an ACME authority acme_url without an effective server-side destination restriction and trigger AcmeHandler.setup_acme_client to make backend requests. An attacker could target cloud instance metadata or internal services from Lemur network context, potentially obtaining credentials available to the host. The advisory also identifies creator-equality authorization behavior that could preserve access to certificate key material after ownership or role changes, with insufficient export_private_key audit context to distinguish that access path. Together, the acme_url server-side request forgery and authorization weakness could expose cloud credentials and long-lived PKI private-key access. The fix adds ACME_DIRECTORY_HOST_ALLOWLIST validation and enriches key-export audit events with creator and current-owner context. This issue is fixed in version 1.9.2.	2026-08-18	9.9	CVE-2026-55166

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.1, StrictRolePermission and AuthorityCreatorPermission in lemur/auth/permissions.py call flask_principal.Permission.__init__() with zero Need objects when ADMIN_ONLY_AUTHORITY_CREATION and LEMUR_STRICT_ROLE_ENFORCEMENT are unset because both flags default to False. Flask-Principal Permission.allows() returns True when self.needs is empty, so the .can() authorization gate permits every authenticated identity, including the read-only role. A read-only user can access POST /api/1/authorities, POST /api/1/certificates/upload, POST /api/1/pending_certificates/upload, POST /api/1/notifications, PUT or DELETE /api/1/notifications/, and POST /api/1/domains to create root Certificate Authorities, upload arbitrary certificates, create or edit notifications that reach an SSRF sink, and create domain entries. Explicitly setting either flag to False continues to opt into the permissive behavior. This issue is fixed in version 1.9.1.	2026-08-18	8.8	CVE-2026-48508
Netflix--lemur	Lemur manages TLS certificate creation. From 0.5.0 until 1.9.3, certificate create, upload, and edit requests accepted replaces[] or replacements identifiers that AssociatedCertificateSchema resolved with fetch_objects without a CertificatePermission check. Assigning those objects to Certificate.replaces invoked an append listener that disabled the victim certificate notifications and marked it as replaced. The victim was then excluded from get_all_pending_reissue, and certificate_rotate could deploy the attacker certificate to endpoints serving the victim. An authenticated non-read-only user could target certificates for which the user had no ownership or role, suppress lifecycle automation, and cause fleet-wide TLS disruption or unauthorized substitution. The fix authorizes every referenced replacement certificate before mutation. This issue is fixed in version 1.9.3.	2026-08-18	8.1	CVE-2026-71308
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.3, an authority-role member could update acme_url through PUT /api/1/authorities/ without revalidation and direct setup_acme_client_no_retry to an attacker-controlled ACME server. ACME directory and order responses contain newNonce, newOrder, authorizations, and finalize URLs chosen by that server. The Lemur ClientV2 followed those URLs without requiring their host to match the configured directory host, allowing JWS-signed requests to internal services or cloud metadata endpoints. The issue required an ACME authority and a user authorized for that authority, but did not require global administrator privileges. The fix revalidates updates and introduces PinnedClientNetwork to enforce a single allowed host for the complete ACME flow. This issue is fixed in version 1.9.3.	2026-08-18	7.4	CVE-2026-70666
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.3, _validate_acme_url enforced ACME_DIRECTORY_HOST_ALLOWLIST when an authority was created, but PUT /api/1/authorities/ passed options to lemur/authorities/service.py without applying the same check. A user holding an authority role could replace the stored acme_url with an internal service or instance-metadata URL such as 169.254.169.254. The next issuance operation loaded that value and passed it to ClientV2.get_directory, causing an outbound request from the Lemur backend. This bypassed the creation-time mitigation for CVE-2026-55166 and could expose internal services or cloud metadata. The fix revalidates acme_url whenever authority options are updated. This issue is fixed in version 1.9.3.	2026-08-18	7.7	CVE-2026-71303
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.3, GET /api/1/destinations and GET /api/1/destinations/ relied only on authentication while sibling write handlers required admin_permission. DestinationOutputSchema returned raw options and copied them into pluginOptions without redacting sensitive values. The sftp-destination plugin stored password and privateKeyPass values in plaintext, allowing even a read-only user to retrieve credentials for remote certificate-deployment hosts. The exposed credentials could permit direct access to SFTP systems and TLS material outside the Lemur security boundary. The fix requires administrator permission for destination reads and redacts options marked sensitive. This issue is fixed in version 1.9.3.	2026-08-18	7.7	CVE-2026-71307
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.3, POST /api/1/certificates/upload allowed a non-read-only user to create a duplicate row using another certificate body, authority_id, serial, or external_id without requiring permission on the underlying authority. PUT /api/1/certificates/revoke authorized the caller against only the selected Lemur row, so the creator of the duplicate bypassed CertificatePermission. The duplicate had no cert.endpoints, which also bypassed the safeguard that prevents revocation of deployed certificates. Issuer plugins then revoked the real CA-side certificate using certificate.body or external_id under the stored authority credentials. An attacker could therefore revoke arbitrary managed certificates and cause fleet-wide TLS denial of service.	2026-08-18	7.3	CVE-2026-71417

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The fix rejects duplicate authority_id and serial identities, requires authority access on upload, and checks every matching row during revocation. This issue is fixed in version 1.9.3.			
netty--netty	Netty is an asynchronous, event-driven network application framework. Prior to 4.1.137.Final and 4.2.17.Final, io.netty.handler.codec.sctp.SctpMessageCompletionHandler limits incomplete messages and fragment counts but not maxBufferedBytes, allowing unauthenticated peers to exhaust memory with large SCTP fragments. This issue is fixed in versions 4.1.137.Final and 4.2.17.Final.	2026-08-17	7.5	CVE-2026-59902
netty--netty	Netty (io.netty:netty-handler) versions from 4.2.0.Final through 4.2.16.Final and versions through 4.1.136.Final disable TLS hostname verification on the SslProvider.OPENSSL client path when a plain (non-extended) X509TrustManager is used and Unsafe-based trust-manager wrapping is unavailable (Java 25+). In this configuration the OpenSSL client does not perform hostname verification, allowing a man-in-the-middle attacker to present a certificate issued for a different hostname that is accepted without validation. Fixed in 4.2.17.Final and 4.1.137.Final.	2026-08-22	7.5	CVE-2026-62243
Nexcess--Starter Templates by Kadence WP	Unauthenticated Denial of Service Attack in Starter Templates by Kadence WP <= 2.3.3 versions.	2026-08-18	7.5	CVE-2026-73997
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. Nezha versions 1.14.13 through 1.14.14 and 2.0.0 through 2.0.9 do not bind stream identifiers created by CreateStream in service/rpc/io_stream.go to their creating user, and 'GET /ws/terminal/:id' and 'GET /ws/file/:id' only check whether the supplied UUID exists. An authenticated RoleMember who obtains a live stream UUID from logs, browser history, referer data, or telemetry can attach to another user's terminal or file-manager session, read and write target-server files, and execute shell commands. This issue is fixed in version 2.0.10.	2026-08-21	9.9	CVE-2026-62283
nicolargo--glances	Glances is an open-source system cross-platform monitoring tool. From 4.5.2 until 4.5.6, _sanitize_mustache_dict() in glances/actions.py skips nested list and dictionary strings such as process cmdline values, allowing pipe characters to survive chevron.render() and be executed by secure_popen() through administrator-configured action templates. This issue is fixed in 4.5.6.	2026-08-17	8.8	CVE-2026-62982
nltk--nltk	NLTK before 3.10.3 contains a remote code execution vulnerability in AllowlistUnpickler that validates only the pickle module string and not the global name, allowing attackers to resolve dotted names by attribute traversal to callables outside the allowlisted namespace. Attackers can craft untrusted transition-parser models that execute arbitrary commands when TransitionParser.parse loads the model through allowlisted_pickle_load.	2026-08-22	8.8	CVE-2026-71513
nltk--nltk	NLTK versions before 3.10.2 contain a symlink-based sandbox bypass in FramenetCorpusReader that allows attackers to read arbitrary XML files outside the corpus root. Attackers can place symlinks with names containing no path separators inside the corpus subdirectory, which pass the path validation guard and are resolved to files outside the intended corpus root when accessed via frame_by_name(), _lu_file(), or doc() methods.	2026-08-22	7.5	CVE-2026-62384
nltk--nltk	NLTK versions before 3.10.0 default to ENFORCE=False in pathsec.py, causing all security validation functions to emit warnings instead of raising exceptions. Attackers can bypass path traversal and pickle deserialization protections by exploiting the disabled security controls that are only active when manually enabled.	2026-08-22	7.5	CVE-2026-62388
nltk--nltk	NLTK before 3.9.3 fails to verify file integrity after downloading packages and before extraction in the downloader module. Attackers can perform man-in-the-middle attacks or DNS poisoning to inject malicious package contents that are extracted without validation.	2026-08-22	7.1	CVE-2026-63310
nltk--nltk	NLTK before 3.10.0 contains an arbitrary local file read vulnerability in StreamBackedCorpusView that bypasses pathsec.ENFORCE by calling builtins.open() directly instead of pathsec.open(). Attackers who control the fileid argument can read arbitrary local files regardless of the ENFORCE setting, including sensitive system files and application credentials.	2026-08-22	7.5	CVE-2026-63312
nltk--nltk	NLTK versions before 3.9.4 contain an unbounded recursion vulnerability in JSONTaggedDecoder.decode_obj() that allows attackers to cause denial of service by supplying deeply nested JSON structures. Attackers can craft JSON payloads exceeding the recursion limit to trigger an unhandled RecursionError that crashes the Python process.	2026-08-22	7.5	CVE-2026-66393

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nltk--nltk	The URLS regular expression in nltk/tokenize/casual.py, compiled into TweetTokenizer.WORD_RE and applied by TweetTokenizer.tokenize, contains a naked-domain branch whose domain-label prefix [a-z0-9]+(?:[.\\-][a-z0-9]+)* is unbounded. Input consisting of many alternating label separators can be partitioned in exponentially many ways, and because the branch also requires a trailing top-level domain that such input never supplies, the engine explores those partitions before failing at each offset. A few kilobytes of input therefore consumes seconds to minutes of single-threaded CPU, and the HANG_RE substitution performed before matching does not collapse the pattern. TweetTokenizer is intended for tokenizing untrusted social-media text, so any service that applies it, or the module-level casual_tokenize, to submitted text can be stalled per request without authentication. Version 3.10.1 bounds the label repetition.	2026-08-20	7.5	CVE-2026-72818
notepad-plus-plus--notepad-plus-plus	Notepad++ is a free and open-source source code editor. Prior to 8.9.7, the WinGup decompress function joins untrusted ZIP entry names to unzipDestTo without canonical containment validation, allowing an entry such as ../mimeTools/mimeTools.dll to overwrite a DLL in a sibling plugin directory and execute attacker-controlled code when Notepad++ next loads that plugin. This issue is fixed in version 8.9.7.	2026-08-17	8.1	CVE-2026-57233
notepad-plus-plus--notepad-plus-plus	Notepad++ is a free and open-source source code editor. Prior to 8.9.7, the expandNppEnvironmentStrs function in PowerEditor/src/WinControls/StaticDialog/RunDlg/RunDlg.cpp copies a Notepad++ variable name between \$(and) into the fixed-size wchar_t str[MAX_PATH] stack buffer without bounding the m loop index, allowing a name of 260 or more characters to corrupt adjacent stack data, terminate the process through _report_gsfailure, and potentially execute code. This issue is fixed in version 8.9.7.	2026-08-17	7.8	CVE-2026-54758
NotificationX--NotificationX Pro	Unauthenticated Cross Site Scripting (XSS) in NotificationX Pro <= 3.1.4 versions.	2026-08-20	7.1	CVE-2026-68564
NVIDIA--Cumulus Linux GA	NVIDIA Cumulus Linux contains a vulnerability in the user management component, where an unprivileged user could use improper privilege management on the system. A successful exploit of this vulnerability might lead to escalation of privileges.	2026-08-18	7.8	CVE-2026-24183
NVIDIA--Cumulus Linux GA	NVIDIA Cumulus Linux contains a vulnerability in the Link Layer Discovery Protocol (LLDP) daemon component, where an unauthenticated attacker on an adjacent network could cause buffer overflow by sending crafted LLDP frames. A successful exploit of this vulnerability might lead to code execution.	2026-08-18	7.5	CVE-2026-24184
NVIDIA--NVOS	NVIDIA NVOS for network switches contains a vulnerability in the secure shell (SSH) server configuration component while PKA-only mode is enabled, where an administrator could inadvertently enable an alternative authentication path. If best practices for replacing the default password as recommended by NVIDIA are not followed, this alternative authentication path might lead to unauthorized access. A successful exploit of this vulnerability might lead to escalation of privileges.	2026-08-18	7.1	CVE-2026-24185
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker could cause path traversal. A successful exploit might lead to denial of service.	2026-08-18	9.8	CVE-2026-47627
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker could cause an allocation of resources without limits. A successful exploit might lead to denial of service.	2026-08-18	7.5	CVE-2026-47628
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker could cause improper input validation. A successful exploit might lead to denial of service.	2026-08-18	7.5	CVE-2026-47629
ohmyzsh--ohmyzsh	Oh My Zsh is a community-driven framework for managing Zsh configuration. Prior to 2026-05-28, the dotenv plugin in plugins/dotenv/dotenv.plugin.zsh passes ZSH_DOTENV_FILE to source after a directory change into a folder containing a .env file, allowing syntactically valid shell commands in the file to execute with the current account's privileges, including without a prompt when ZSH_DOTENV_PROMPT=false or after the default prompt accepts an empty Enter response. This issue is fixed in versions released after 2026-05-28.	2026-08-18	8.8	CVE-2026-50187
omnigent-ai--omnigent	Omnigent is an open-source AI agent framework and meta-harness for orchestrating coding agents. Prior to 0.3.0, PUT /sessions/{session_id}/agent checks LEVEL_EDIT permission for a session but does not reject a bound shared or template agent whose agent.session_id is None. An authenticated user with edit access to a session can replace that shared agent bundle through omnigent/server/routes/sessions.py, add a stdio MCP server, and cause later sessions that use the shared agent to launch an attacker-controlled command through omnigent/tools/mcp.py. The command executes with the Omnigent	2026-08-21	9	CVE-2026-62674

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	runner process permissions and can expose files, credentials, workspace data, internal services, and runner availability. This issue is fixed in version 0.3.0.			
omnigent-ai--omnigent	Omnigent is an open-source AI agent framework and meta-harness for orchestrating coding agents. Prior to 0.3.0, multipart POST /v1/sessions accepts an authenticated user's agent bundle and omnigent/server/bundles.py validate_agent_bundle does not reject a tools..callable dotted Python path. omnigent/runner/tool_dispatch.py _resolve_spec_callable imports the specified module and _execute_spec_callable_tool invokes the resolved function, allowing a bundle to select subprocess.check_output and execute a local command with the runner process permissions. This can expose runner files, environment variables, credentials, workspace data, internal services, and availability without administrator access. This issue is fixed in version 0.3.0.	2026-08-21	8.8	CVE-2026-62675
omnigent-ai--omnigent	Omnigent is an open-source AI agent framework and meta-harness for orchestrating coding agents. Prior to 0.3.0, an authenticated user can upload a session-scoped agent bundle with an absolute or traversal-containing os_env.cwd value because omnigent/spec/parser.py stores the value verbatim and omnigent/spec/validator.py does not constrain it. On a runner where OMNIGENT_RUNNER_WORKSPACE is unset, omnigent/runner/resource_registry.py preserves the attacker-controlled path and omnigent/inner/os_env.py uses the resolved path as the environment root and copytree source. The _assert_within_cwd check then treats that attacker-selected root as trusted, allowing sys_os_read, write, edit, and shell tools to access runner files and environment secrets outside the intended workspace. This issue is fixed in version 0.3.0.	2026-08-21	8.8	CVE-2026-62677
omnigent-ai--omnigent	Omnigent is an open-source AI agent framework and meta-harness for orchestrating coding agents. Prior to 0.3.0, the shared shell-command parser in omnigent/policies/builtins/_shell.py fails to recognize combined interpreter flags, the timeout, nice, setsid, and stdbuf wrappers, command substitutions, and a single background control operator. A gated git push or gh write hidden with these forms produces no parsed operation, causing the github.py write_repos and write_branches allowlist and the working_dir.py workspace confinement policies to abstain and allow the command. An authenticated or prompt-injected agent can therefore push to an unauthorized repository or branch or escape the intended workspace. This issue is fixed in version 0.3.0.	2026-08-21	7.1	CVE-2026-62676
OnGres--StackGres	privilege escalation in StackGres operator allows a low-privilege tenant who owns a database to gain administrator privileges	2026-08-23	9.9	CVE-2026-78155
ONNX--ONNX	In ONNX before 1.21.0, the 'save_external_data' function builds the external-data file path from the model's external_data location field and opens it for writing without 'O_NOFOLLOW/O_EXCL', after a non-atomic 'os.path.isfile()' check. A local attacker with write access to the directory where a victim serializes external data can deterministically pre-plant a symlink that is being followed, causing the victim's write to append to any file the victim can write, e.g. ~/.ssh/authorized_keys, cron files, or application configs. Fixed in 1.21.0.	2026-08-21	7.1	CVE-2026-49114
onyx-dot-app--onyx	Onyx is an open-source AI platform. Prior to 3.1.10, 3.2.14, and 4.0.0, Onyx's GET /api/mcp/servers and GET /api/mcp/servers/persona/{persona_id} endpoints expose another user's OAuth Authorization header because OnyxTokenStorage.set_tokens and OnyxTokenStorage.set_client_info in backend/onyx/server/features/mcp/api.py copy per-user tokens into a shared admin MCPConnectionConfig row and _db_mcp_server_to_api_mcp_server returns that row through auth_template.headers to any BASIC_ACCESS user. This issue is fixed in versions 3.1.10, 3.2.14, and 4.0.0.	2026-08-17	9.6	CVE-2026-71424
OP-Engineering--link-preview-js	Link Preview JS extracts web links information. Prior to 4.0.4, the resolvedDNSHost mitigation in index.ts validates one resolved IP address but fetches the original hostname, allowing an attacker-controlled DNS server to return a public address during validation and a loopback or internal address during the final connection. This DNS rebinding condition bypasses the SSRF protection and can cause the server-side preview fetch to reach internal HTTP resources. Redirect handling is affected by the same validation-to-fetch mismatch. This issue is fixed in version 4.0.4.	2026-08-20	7.5	CVE-2026-61704
Open5GS--Open5GS	A security vulnerability has been detected in Open5GS 2.8.0. Affected by this issue is the function hss_ogs_diam_s6a_air_cb of the file src/hss/hss-s6a-path.c of the component S6a Authentication-Information-Request Handler. Such manipulation of the argument Visited-PLMN-Id leads to heap-based buffer overflow. The attack may be performed from remote. The name of the patch is	2026-08-23	7.4	CVE-2026-78156

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a9c82ee0b590d76a581b0580cb46b598984e2392. A patch should be applied to remediate this issue.			
OpenIDC-- mod_auth_openidc	mod_auth_openidc is an OpenID Certified authentication and authorization module for the Apache 2.x HTTP server that implements the OpenID Connect Relying Party functionality. Prior to 2.4.19.4, an out-of-bounds read and a one-byte out-of-bounds write exist in the state-cookie parser of `mod_auth_openidc`. The issue is fixed in version 2.4.19.4 by stopping the scan at the string terminator so a value-less token is rejected. No in-product workarounds are available. As a stop-gap, an upstream reverse proxy or WAF that rejects or normalizes malformed `Cookie` headers (tokens lacking `=`) can reduce exposure, but upgrading is the recommended remediation.	2026-08-21	7.5	CVE-2026-54789
OpenSearch-- OpenSearch Dashboards	Improper input validation in the capabilities route handler in OpenSearch Dashboards - the size of the request payload is not bounded - might allow remote attackers to cause a denial of service via a crafted HTTP request.	2026-08-18	7.5	CVE-2026-75897
openshift-metal3-- fakefish	FakeFish handles incoming credentials by passing them down to scripts. This works for real hardware because in the end it's up to the BMC to validate them. However, KubeVirt relies on a KUBECONFIG file mounted to the container and completely ignores the credentials. This allows any user of the cluster to control VMs of the user that created fakefish, power them on and off, and mount arbitrary CD images to them.	2026-08-17	9.3	CVE-2026-71566
openshift-metal3-- fakefish	In openshift-metal3/fakefish there is a repeated pattern in some of the scripts where shell variables are injected without quoting them either into command lines or into manifests. This mostly applies to the Image URL and BMC credentials (which are not verified by FakeFish).	2026-08-17	7.7	CVE-2026-71567
OpnForm-- OpnForm	OpnForm derives editable-submission secrets from sequential row identifiers using Hashids with an empty default salt, allowing unauthenticated attackers to compute hashes for any submission. Attackers can read other respondents' full submission data through the submission-fetch endpoint or overwrite submissions by supplying predicted hashes to the answer endpoint.	2026-08-17	9.1	CVE-2026-75106
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data as well as unauthorized update, insert or delete access to some of Helidon accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	9.3	CVE-2026-71065
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-71074
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-71152
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-71164
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon	2026-08-18	9.4	CVE-2026-71166

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 9.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L).			
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 9.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L).	2026-08-18	9.4	CVE-2026-71167
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-73865
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-73866
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-73905
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-73912
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-73916
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-73917
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via	2026-08-18	9.4	CVE-2026-73920

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 9.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L).			
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 1.4.20. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-73921
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 1.4.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-73922
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 1.4.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-73924
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L).	2026-08-18	9.9	CVE-2026-73930
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-71110
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data as well as unauthorized update, insert or delete access to some of Helidon accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	8.5	CVE-2026-71155
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data as well as unauthorized update, insert or delete access to some of Helidon	2026-08-18	8.2	CVE-2026-71159

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).			
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 1.4.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).	2026-08-18	8.2	CVE-2026-73925
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L).	2026-08-18	8.3	CVE-2026-73929
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L).	2026-08-18	8.3	CVE-2026-73931
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP/2 to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon and unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H).	2026-08-18	8.2	CVE-2026-73937
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.20. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data. CVSS 3.1 Base Score 8.6 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N).	2026-08-18	8.6	CVE-2026-73939
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data as well as unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-60915
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-70908
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 1.4.20. Easily exploitable vulnerability allows unauthenticated attacker with network access via	2026-08-18	7.5	CVE-2026-71153

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).			
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-71158
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in takeover of Helidon. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-71160
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).	2026-08-18	7.2	CVE-2026-73875
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).	2026-08-18	7.2	CVE-2026-73876
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-73878
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	2026-08-18	7.5	CVE-2026-73879
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-73882
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-73883

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-73884
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).	2026-08-18	7.2	CVE-2026-73885
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).	2026-08-18	7.2	CVE-2026-73886
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP/2 to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-73887
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP/2 to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-73890
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2026-08-18	7.3	CVE-2026-73891
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2026-08-18	7.3	CVE-2026-73894
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-73902

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	2026-08-18	7.5	CVE-2026-73903
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-73907
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-73908
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-73915
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2026-08-18	7.3	CVE-2026-73918
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.20. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-73927
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).	2026-08-18	7.2	CVE-2026-73928
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2026-08-18	7.3	CVE-2026-73933

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP/2 to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-73934
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP/2 to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-73935
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Helidon. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-73936
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-73938
Oracle Corporation--JD Edwards EnterpriseOne Orchestrator	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product of Oracle JD Edwards (component: E1 IOT Orchestrator Security). Supported versions that are affected are 9.2.0.0-9.2.26.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise JD Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Orchestrator. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-61265
Oracle Corporation--JD Edwards EnterpriseOne Orchestrator	Vulnerability in the JD Edwards EnterpriseOne Orchestrator product of Oracle JD Edwards (component: E1 IOT Orchestrator Security). Supported versions that are affected are 9.2.0.0-9.2.26.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Orchestrator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Orchestrator accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Orchestrator accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-61270
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime SEC). Supported versions that are affected are 9.2.0.0-9.2.26.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-61272
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Business Logic Infra SEC). Supported versions that are affected are 9.2.0.0-9.2.26.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Tools accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-61268

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Installation Security). Supported versions that are affected are 9.2.0.0-9.2.26.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61273
Oracle Corporation--JD Edwards EnterpriseOne US Payroll	Vulnerability in the JD Edwards EnterpriseOne US Payroll product of Oracle JD Edwards (component: Payroll). The supported version that is affected is 9.2. Difficult to exploit vulnerability allows low privileged attacker with network access via JDENET to compromise JD Edwards EnterpriseOne US Payroll. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne US Payroll. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-60956
Oracle Corporation--MySQL Cluster	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: NDB Operator). Supported versions that are affected are 8.0.0-8.0.47, 8.4.0-8.4.10 and 9.7.0-9.7.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Cluster as well as unauthorized update, insert or delete access to some of MySQL Cluster accessible data. CVSS 3.1 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).	2026-08-18	8.2	CVE-2026-60592
Oracle Corporation--MySQL Cluster	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.0-8.0.48, 8.4.0-8.4.11 and 9.7.0-9.7.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70724
Oracle Corporation--Oracle Access Manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Agent infrastructure). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via SAML to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in takeover of Oracle Access Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70905
Oracle Corporation--Oracle Access Manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in takeover of Oracle Access Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60726
Oracle Corporation--Oracle Advanced Inbound Telephony	Vulnerability in the Oracle Advanced Inbound Telephony product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Advanced Inbound Telephony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Inbound Telephony accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Advanced Inbound Telephony. CVSS 3.1 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L).	2026-08-18	8.2	CVE-2026-70722
Oracle Corporation--Oracle Advanced Inbound Telephony	Vulnerability in the Oracle Advanced Inbound Telephony product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Inbound Telephony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Inbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Inbound Telephony accessible data and unauthorized ability to	2026-08-18	7.6	CVE-2026-70725

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cause a partial denial of service (partial DOS) of Oracle Advanced Inbound Telephony. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).			
Oracle Corporation-- Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Engineering Communication Interface). The supported version that is affected is 6.2.1. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile Engineering Data Management. While the vulnerability is in Oracle Agile Engineering Data Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Agile Engineering Data Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Agile Engineering Data Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.2	CVE-2026-70703
Oracle Corporation-- Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Web Services Security). The supported version that is affected is 6.2.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile Engineering Data Management. Successful attacks of this vulnerability can result in takeover of Oracle Agile Engineering Data Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71052
Oracle Corporation-- Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Web Services Security). The supported version that is affected is 6.2.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile Engineering Data Management. Successful attacks of this vulnerability can result in takeover of Oracle Agile Engineering Data Management. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-71053
Oracle Corporation-- Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Engineering Communication Interface). The supported version that is affected is 6.2.1. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Agile Engineering Data Management executes to compromise Oracle Agile Engineering Data Management. Successful attacks of this vulnerability can result in takeover of Oracle Agile Engineering Data Management. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70691
Oracle Corporation-- Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Engineering Communication Interface). The supported version that is affected is 6.2.1. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Agile Engineering Data Management executes to compromise Oracle Agile Engineering Data Management. Successful attacks of this vulnerability can result in takeover of Oracle Agile Engineering Data Management. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7	CVE-2026-70697
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Security). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-71040
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Application Server). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71039

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: PGC / Excel Plugin). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Agile PLM accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Agile PLM. CVSS 3.1 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	8.1	CVE-2026-71042
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Export). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71044
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Security). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71045
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Security). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Agile PLM executes to compromise Oracle Agile PLM. While the vulnerability is in Oracle Agile PLM, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71046
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Gantt Chart). The supported version that is affected is 9.3.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Agile PLM executes to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7	CVE-2026-71041
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Security). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-71043
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM MCAD Connector. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71067
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM MCAD Connector. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-71068
Oracle Corporation--	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows low privileged attacker with network access	2026-08-18	7.5	CVE-2026-71069

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Agile PLM MCAD Connector	via HTTP to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM MCAD Connector. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Application Testing Suite	Vulnerability in Oracle Application Testing Suite. The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Application Testing Suite accessible data as well as unauthorized access to critical data or complete access to all Oracle Application Testing Suite accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-70862
Oracle Corporation-- Oracle Application Testing Suite	Vulnerability in Oracle Application Testing Suite. The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker having Load Testing for Web Apps privilege with network access via HTTPS to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in takeover of Oracle Application Testing Suite. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70863
Oracle Corporation-- Oracle Application Testing Suite	Vulnerability in Oracle Application Testing Suite. The supported version that is affected is 13.3.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in takeover of Oracle Application Testing Suite. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-70868
Oracle Corporation-- Oracle Application Testing Suite	Vulnerability in Oracle Application Testing Suite. The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker having Load Testing for Web Apps privilege with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Testing Suite, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Application Testing Suite accessible data as well as unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-70864
Oracle Corporation-- Oracle Application Testing Suite	Vulnerability in Oracle Application Testing Suite. The supported version that is affected is 13.3.0.1. Difficult to exploit vulnerability allows low privileged attacker having Load Testing for Web Apps privilege with network access via HTTPS to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in takeover of Oracle Application Testing Suite. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70865
Oracle Corporation-- Oracle Application Testing Suite	Vulnerability in Oracle Application Testing Suite. The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker having Load Testing for Web Apps privilege with logon to the infrastructure where Oracle Application Testing Suite executes to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in takeover of Oracle Application Testing Suite. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-70866
Oracle Corporation-- Oracle Application Testing Suite	Vulnerability in Oracle Application Testing Suite. The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Application Testing Suite executes to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Application Testing Suite accessible data as well as unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70867

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Applications DBA	Vulnerability in the Oracle Applications DBA product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications DBA. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications DBA accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications DBA. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	7.1	CVE-2026-70680
Oracle Corporation-- Oracle Applications DBA	Vulnerability in the Oracle Applications DBA product of Oracle E-Business Suite (component: JRI and other Java utils). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications DBA. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Applications DBA. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70681
Oracle Corporation-- Oracle Applications Platform Engineering	Vulnerability in the Oracle Applications Platform Engineering product of Oracle E-Business Suite (component: Valid Session). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Oracle Applications Platform Engineering. Successful attacks of this vulnerability can result in takeover of Oracle Applications Platform Engineering. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-70795
Oracle Corporation-- Oracle Autonomous Health Framework	Vulnerability in Oracle Autonomous Health Framework (component: Trace File Analyzer). Supported versions that are affected are 26-26.1.0, 26.2.0, 26.3.1, 26.5.0 and 26.5.2. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Autonomous Health Framework executes to compromise Oracle Autonomous Health Framework. Successful attacks of this vulnerability can result in takeover of Oracle Autonomous Health Framework. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70715
Oracle Corporation-- Oracle Autonomous Health Framework	Vulnerability in Oracle Autonomous Health Framework (component: Trace File Analyzer). Supported versions that are affected are 26-26.1.0, 26.2.0, 26.3.1, 26.5.0 and 26.5.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Autonomous Health Framework. While the vulnerability is in Oracle Autonomous Health Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Autonomous Health Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Autonomous Health Framework accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	8.5	CVE-2026-70728
Oracle Corporation-- Oracle Autonomous Health Framework	Vulnerability in Oracle Autonomous Health Framework (component: Trace File Analyzer). Supported versions that are affected are 26-26.1.0, 26.2.0, 26.3.1, 26.5.0 and 26.5.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Autonomous Health Framework executes to compromise Oracle Autonomous Health Framework. While the vulnerability is in Oracle Autonomous Health Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Autonomous Health Framework accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Autonomous Health Framework. CVSS 3.1 Base Score 8.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H).	2026-08-18	8.4	CVE-2026-70731
Oracle Corporation-- Oracle Autonomous Health Framework	Vulnerability in Oracle Autonomous Health Framework (component: Cluster Health Analyzer). Supported versions that are affected are 26-26.1.0, 26.2.0, 26.3.1, 26.5.0 and 26.5.2. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Autonomous Health Framework executes to compromise Oracle Autonomous Health Framework. While the vulnerability is in Oracle Autonomous Health Framework, attacks may significantly impact additional products (scope	2026-08-18	7.7	CVE-2026-70717

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Autonomous Health Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Autonomous Health Framework accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Autonomous Health Framework	Vulnerability in Oracle Autonomous Health Framework (component: Trace File Analyzer). Supported versions that are affected are 26-26.1.0, 26.2.0, 26.3.1, 26.5.0 and 26.5.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Autonomous Health Framework executes to compromise Oracle Autonomous Health Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Autonomous Health Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Autonomous Health Framework accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Autonomous Health Framework. CVSS 3.1 Base Score 7.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:N/I:H/A:H).	2026-08-18	7.4	CVE-2026-70734
Oracle Corporation-- Oracle BI Publisher	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Service API). Supported versions that are affected are 8.2.0.0.0 and 26.1.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via SOAP to compromise Oracle BI Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-71059
Oracle Corporation-- Oracle BI Publisher	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: BI Platform Security). Supported versions that are affected are 8.2.0.0.0, 12.2.1.4.0 and 26.01.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle BI Publisher accessible data as well as unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L).	2026-08-18	8.3	CVE-2026-61305
Oracle Corporation-- Oracle BI Publisher	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: BI Platform Security). Supported versions that are affected are 8.2.0.0.0, 12.2.1.4.0 and 26.1.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 8.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L).	2026-08-18	8.5	CVE-2026-71057
Oracle Corporation-- Oracle BI Publisher	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Service API). Supported versions that are affected are 8.2.0.0.0, 12.2.1.4.0 and 26.01.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71058
Oracle Corporation-- Oracle Bills of Material	Vulnerability in the Oracle Bills of Material product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Bills of Material. While the vulnerability is in Oracle Bills of Material, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Bills of Material. CVSS 3.1 Base Score 8.5	2026-08-18	8.5	CVE-2026-70718

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Pod Admin). Supported versions that are affected are 8.2.0.0.0 and 26.01.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	8.2	CVE-2026-61302
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Platform Security). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71055
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: BI Platform Security). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L).	2026-08-18	8.3	CVE-2026-71095
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: BI Platform Security). Supported versions that are affected are 8.2.0.0.0, 12.2.1.4.0 and 26.01.0.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Business Intelligence Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.2	CVE-2026-71096
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Platform Security). The supported version that is affected is 26.01.0.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8	CVE-2026-71122
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: BI Search). Supported versions that are affected are 8.2.0.0.0, 12.2.1.4.0 and 26.01.0.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-71056

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: BI Platform Security). Supported versions that are affected are 8.2.0.0.0 and 26.01.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-71061
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Presentation Services). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Business Intelligence Enterprise Edition executes to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.3	CVE-2026-71094
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Platform Security). The supported version that is affected is 26.01.0.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Business Intelligence Enterprise Edition executes to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-71097
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Platform Security). The supported version that is affected is 26.01.0.0.0. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Business Intelligence Enterprise Edition executes to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7	CVE-2026-71098
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Answers). The supported version that is affected is 26.01.0.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-71099
Oracle Corporation-- Oracle Business Intelligence Enterprise Edition	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Server). Supported versions that are affected are 8.2.0.0.0 and 26.01.0.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-71107
Oracle Corporation-- Oracle Call Center Technology	Vulnerability in the Oracle Call Center Technology product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Call Center Technology. While the vulnerability is in Oracle Call Center Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Call Center Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Call Center Technology accessible data. CVSS 3.1 Base	2026-08-18	8.5	CVE-2026-70807

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).			
Oracle Corporation-- Oracle Call Center Technology	Vulnerability in the Oracle Call Center Technology product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Call Center Technology. Successful attacks of this vulnerability can result in takeover of Oracle Call Center Technology. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70812
Oracle Corporation-- Oracle Call Center Technology	Vulnerability in the Oracle Call Center Technology product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Call Center Technology. Successful attacks of this vulnerability can result in takeover of Oracle Call Center Technology. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70813
Oracle Corporation-- Oracle Call Center Technology	Vulnerability in the Oracle Call Center Technology product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Call Center Technology. Successful attacks of this vulnerability can result in takeover of Oracle Call Center Technology. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-70814
Oracle Corporation-- Oracle Call Center Technology	Vulnerability in the Oracle Call Center Technology product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Call Center Technology. Successful attacks of this vulnerability can result in takeover of Oracle Call Center Technology. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-70820
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-70976
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-70977
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data.	2026-08-18	9.1	CVE-2026-70978

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-70979
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9	CVE-2026-70980
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-70981
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-70984
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H).	2026-08-18	9.1	CVE-2026-70994
Oracle Corporation-- Oracle Commerce	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable	2026-08-18	9.8	CVE-2026-70995

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Guided Search / Oracle Commerce Experience Manager	vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 9.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H).	2026-08-18	9.1	CVE-2026-70997
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	9.3	CVE-2026-70998
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-71014
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-71015
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce	2026-08-18	9.1	CVE-2026-71026

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-71036
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).	2026-08-18	9.3	CVE-2026-71037
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager as well as unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).	2026-08-18	8.2	CVE-2026-70993
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	8.6	CVE-2026-70996
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1	2026-08-18	8.1	CVE-2026-70999

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-71000
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:N).	2026-08-18	8.5	CVE-2026-71002
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-71016
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-71018
Oracle Corporation-- Oracle Commerce Guided Search /	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Forge). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle	2026-08-18	8.2	CVE-2026-71024

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Commerce Experience Manager	Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Forge). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-71035
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70985
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70986
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70987
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70988
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Commerce Guided Search / Oracle Commerce Experience Manager	2026-08-18	7	CVE-2026-70992

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Experience Manager	executes to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	7.1	CVE-2026-71003
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-71009
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Commerce Guided Search / Oracle Commerce Experience Manager executes to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-71010
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	7.1	CVE-2026-71012
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base	2026-08-18	7.6	CVE-2026-71020

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-71021
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Workbench). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-71022
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	2026-08-18	7.5	CVE-2026-71023
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-71027
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Commerce Guided Search / Oracle Commerce Experience Manager executes to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Guided Search / Oracle Commerce Experience Manager. CVSS	2026-08-18	7.8	CVE-2026-71028

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).	2026-08-18	7.2	CVE-2026-71030
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N).	2026-08-18	7.2	CVE-2026-71032
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Forge). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via SOAP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-71034
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-71038
Oracle Corporation-- Oracle Commerce Platform	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Platform. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70953
Oracle Corporation-- Oracle Commerce Platform	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Platform. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70954

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Commerce Platform	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Dynamo Application Framework). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Commerce Platform executes to compromise Oracle Commerce Platform. Successful attacks of this vulnerability can result in takeover of Oracle Commerce Platform. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70955
Oracle Corporation-- Oracle Communications Unified Inventory Management	Vulnerability in the Oracle Communications Unified Inventory Management product of Oracle Communications (component: Security Component). Supported versions that are affected are 7.5.0-7.5.1, 7.6.0-7.8.0 and 8.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Unified Inventory Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Communications Unified Inventory Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-71142
Oracle Corporation-- Oracle Communications Unified Inventory Management	Vulnerability in the Oracle Communications Unified Inventory Management product of Oracle Communications (component: Third Party). Supported versions that are affected are 7.5.0, 7.5.1, 7.6.0-7.8.0 and 8.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Communications Unified Inventory Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Communications Unified Inventory Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Communications Unified Inventory Management accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-71143
Oracle Corporation-- Oracle Complex Maintenance, Repair and Overhaul	Vulnerability in the Oracle Complex Maintenance, Repair and Overhaul product of Oracle E-Business Suite (component: Production). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair and Overhaul. While the vulnerability is in Oracle Complex Maintenance, Repair and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Complex Maintenance, Repair and Overhaul accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Complex Maintenance, Repair and Overhaul. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:L).	2026-08-18	7.1	CVE-2026-61306
Oracle Corporation-- Oracle Cost Management	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in takeover of Oracle Cost Management. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-62540
Oracle Corporation-- Oracle Customer Care	Vulnerability in the Oracle Customer Care product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Customer Care. While the vulnerability is in Oracle Customer Care, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Customer Care accessible data as well as unauthorized access to critical data or complete access to all Oracle Customer Care accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-62607
Oracle Corporation-- Oracle Customer Care	Vulnerability in the Oracle Customer Care product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Customer Care. Successful attacks require human interaction from a person other than the attacker and while the	2026-08-18	8.7	CVE-2026-70778

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability is in Oracle Customer Care, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Customer Care accessible data as well as unauthorized access to critical data or complete access to all Oracle Customer Care accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Customers Online	Vulnerability in the Oracle Customers Online product of Oracle E-Business Suite (component: Customer Tab). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Customers Online. Successful attacks of this vulnerability can result in takeover of Oracle Customers Online. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70747
Oracle Corporation-- Oracle Database Server	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 19.3-19.32, 21.3-21.23 and 23.4.0-23.26.3. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.6	CVE-2026-71063
Oracle Corporation-- Oracle Database Server	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 19.3-19.32, 21.3-21.23 and 23.4.0-23.26.3. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.6	CVE-2026-71064
Oracle Corporation-- Oracle Database Server	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 19.3-19.32, 21.3-21.23 and 23.4.0-23.26.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Portable Clusterware. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Portable Clusterware accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Portable Clusterware. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-71102
Oracle Corporation-- Oracle Database Server	Vulnerability in the RDBMS component of Oracle Database Server. Supported versions that are affected are 23.4.0-23.26.3. Difficult to exploit vulnerability allows low privileged attacker having Authenticated User privilege with network access via Oracle Net to compromise RDBMS. While the vulnerability is in RDBMS, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of RDBMS. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.5	CVE-2026-71062
Oracle Corporation-- Oracle Demand Planning	Vulnerability in the Oracle Demand Planning product of Oracle Supply Chain (component: Internal Operations). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Demand Planning. While the vulnerability is in Oracle Demand Planning, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Demand Planning accessible data as well as unauthorized access to critical data or complete access to all Oracle Demand Planning accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	9.6	CVE-2026-70846
Oracle Corporation--	Vulnerability in the Oracle Demand Planning product of Oracle Supply Chain (component: Internal Operations). Supported versions that are affected are 12.1	2026-08-18	8.2	CVE-2026-70852

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Demand Planning	and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Demand Planning. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Demand Planning accessible data as well as unauthorized update, insert or delete access to some of Oracle Demand Planning accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).			
Oracle Corporation-- Oracle E-Business Tax	Vulnerability in the Oracle E-Business Tax product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle E-Business Tax executes to compromise Oracle E-Business Tax. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle E-Business Tax accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle E-Business Tax. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	7.1	CVE-2026-70806
Oracle Corporation-- Oracle Email Center	Vulnerability in the Oracle Email Center product of Oracle E-Business Suite (component: Message Component). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-62448
Oracle Corporation-- Oracle Enterprise Asset Management	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Linear Asset Management). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Asset Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Asset Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Enterprise Asset Management accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-61296
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Application Config Console). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61284
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Event Management). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Oracle Enterprise Manager Base Platform accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L).	2026-08-18	8.6	CVE-2026-61286
Oracle Corporation--	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Agent Next Gen). Supported versions that are	2026-08-18	8.1	CVE-2026-70684

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Enterprise Manager Base Platform	affected are 13.5 and 24.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Agent Next Gen). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-61300
Oracle Corporation-- Oracle Enterprise Manager for Systems Infrastructure	Vulnerability in the Oracle Enterprise Manager for Systems Infrastructure product of Oracle Enterprise Manager (component: Storage Server Management). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager for Systems Infrastructure. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager for Systems Infrastructure. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70737
Oracle Corporation-- Oracle Enterprise Manager for Systems Infrastructure	Vulnerability in the Oracle Enterprise Manager for Systems Infrastructure product of Oracle Enterprise Manager (component: Agent). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Enterprise Manager for Systems Infrastructure executes to compromise Oracle Enterprise Manager for Systems Infrastructure. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager for Systems Infrastructure. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-60822
Oracle Corporation-- Oracle Essbase	Vulnerability in Oracle Essbase (component: Infrastructure). The supported version that is affected is 21.8.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks of this vulnerability can result in takeover of Oracle Essbase. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70689
Oracle Corporation-- Oracle Essbase	Vulnerability in Oracle Essbase (component: Calculator). The supported version that is affected is 21.8.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Essbase. Successful attacks of this vulnerability can result in takeover of Oracle Essbase. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70688
Oracle Corporation-- Oracle Financial Services Enterprise Case Management	Vulnerability in the Oracle Financial Services Enterprise Case Management product of Oracle Financial Services Applications (component: Web UI). Supported versions that are affected are 8.0.8.2 and 8.1.2.11. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Enterprise Case Management. Successful attacks of this vulnerability can result in takeover of Oracle Financial Services Enterprise Case Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70922
Oracle Corporation-- Oracle Financials Common Modules	Vulnerability in the Oracle Financials Common Modules product of Oracle E-Business Suite (component: Common Components). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials Common Modules. While the vulnerability is in Oracle Financials Common Modules, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financials Common Modules accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-61331

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Financials for Asia/Pacific	Vulnerability in the Oracle Financials for Asia/Pacific product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials for Asia/Pacific. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financials for Asia/Pacific accessible data as well as unauthorized read access to a subset of Oracle Financials for Asia/Pacific accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).	2026-08-18	7.1	CVE-2026-70837
Oracle Corporation-- Oracle Financials for EMEA	Vulnerability in the Oracle Financials for EMEA product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials for EMEA. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financials for EMEA accessible data as well as unauthorized update, insert or delete access to some of Oracle Financials for EMEA accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70816
Oracle Corporation-- Oracle Financials for EMEA	Vulnerability in the Oracle Financials for EMEA product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials for EMEA. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Financials for EMEA accessible data as well as unauthorized update, insert or delete access to some of Oracle Financials for EMEA accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70839
Oracle Corporation-- Oracle Flow Manufacturing	Vulnerability in the Oracle Flow Manufacturing product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Flow Manufacturing. Successful attacks of this vulnerability can result in takeover of Oracle Flow Manufacturing. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-62450
Oracle Corporation-- Oracle Flow Manufacturing	Vulnerability in the Oracle Flow Manufacturing product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Flow Manufacturing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Flow Manufacturing accessible data as well as unauthorized update, insert or delete access to some of Oracle Flow Manufacturing accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70801
Oracle Corporation-- Oracle General Ledger	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in takeover of Oracle General Ledger. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70686
Oracle Corporation-- Oracle General Ledger	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle General Ledger. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:L).	2026-08-18	7.1	CVE-2026-60693
Oracle Corporation--	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with	2026-08-18	7.6	CVE-2026-60748

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle General Ledger	network access via HTTP to compromise Oracle General Ledger. While the vulnerability is in Oracle General Ledger, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle General Ledger accessible data as well as unauthorized update, insert or delete access to some of Oracle General Ledger accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N).			
Oracle Corporation-- Oracle General Ledger	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in takeover of Oracle General Ledger. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-60769
Oracle Corporation-- Oracle General Ledger	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle General Ledger accessible data as well as unauthorized update, insert or delete access to some of Oracle General Ledger accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle General Ledger. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	2026-08-18	7.6	CVE-2026-70764
Oracle Corporation-- Oracle General Ledger	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle General Ledger executes to compromise Oracle General Ledger. While the vulnerability is in Oracle General Ledger, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	7.2	CVE-2026-70796
Oracle Corporation-- Oracle General Ledger	Vulnerability in the Oracle General Ledger product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized read access to a subset of Oracle General Ledger accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle General Ledger. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L).	2026-08-18	7.6	CVE-2026-70803
Oracle Corporation-- Oracle HCM Common Architecture	Vulnerability in the Oracle HCM Common Architecture product of Oracle E-Business Suite (component: Knowledge Integration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle HCM Common Architecture. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HCM Common Architecture accessible data as well as unauthorized update, insert or delete access to some of Oracle HCM Common Architecture accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-70773
Oracle Corporation-- Oracle Hospitality OPERA 5 Property Services	Vulnerability in the Oracle Hospitality OPERA 5 Property Services product of Oracle Hospitality Applications (component: Opera Servlet). Supported versions that are affected are 5.6.28.0-5.6.28.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality OPERA 5 Property Services. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71106

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Hospitality Symphony	Vulnerability in the Oracle Hospitality Symphony product of Oracle Food and Beverage Applications (component: POS). Supported versions that are affected are 19.8-19.8.5, 19.9-19.9.3 and 19.10-19.10.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Symphony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Symphony accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Symphony. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-60591
Oracle Corporation-- Oracle Hospitality Symphony	Vulnerability in the Oracle Hospitality Symphony product of Oracle Food and Beverage Applications (component: POS). Supported versions that are affected are 19.8-19.8.5, 19.9-19.9.3 and 19.10-19.10.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Symphony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Symphony accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-60590
Oracle Corporation-- Oracle HRMS (Netherlands)	Vulnerability in the Oracle HRMS (Netherlands) product of Oracle E-Business Suite (component: Netherlands Payroll). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle HRMS (Netherlands). Successful attacks of this vulnerability can result in takeover of Oracle HRMS (Netherlands). CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-71104
Oracle Corporation-- Oracle HRMS (US)	Vulnerability in the Oracle HRMS (US) product of Oracle E-Business Suite (component: US Payroll - General). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle HRMS (US). While the vulnerability is in Oracle HRMS (US), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle HRMS (US). CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8	CVE-2026-70690
Oracle Corporation-- Oracle HRMS (US)	Vulnerability in the Oracle HRMS (US) product of Oracle E-Business Suite (component: US Payroll Tax Issues). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle HRMS (US) executes to compromise Oracle HRMS (US). Successful attacks of this vulnerability can result in takeover of Oracle HRMS (US). CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-71101
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Calculation Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60858
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Calculation Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-61206
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this	2026-08-18	9.6	CVE-2026-62582

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Calculation Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Calculation Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61276
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Calculation Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-61281
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Calculation Manager. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-61293
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via SFTP to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Calculation Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.2	CVE-2026-62598
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Calculation Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 8.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8	CVE-2026-62602
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Calculation Manager. CVSS 3.1 Base Score 7.1 (Confidentiality and	2026-08-18	7.1	CVE-2026-61259

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).			
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Calculation Manager. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L).	2026-08-18	7.2	CVE-2026-62459
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-62571
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Calculation Manager accessible data as well as unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Calculation Manager. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:L).	2026-08-18	7	CVE-2026-70676
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-70678
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 7.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	7.9	CVE-2026-70685
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with	2026-08-18	7.1	CVE-2026-70705

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Calculation Manager	logon to the infrastructure where Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Hyperion Data Relationship Management. While the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	10	CVE-2026-70880
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70871
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-70872
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70873
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Hyperion Data Relationship Management. While the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.1	CVE-2026-70876
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-70883

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation--Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via SOAP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-70884
Oracle Corporation--Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Web Client - Unicode). The supported version that is affected is 11.2.23.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	8.2	CVE-2026-70870
Oracle Corporation--Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70874
Oracle Corporation--Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70877
Oracle Corporation--Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70878
Oracle Corporation--Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70881
Oracle Corporation--Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in	2026-08-18	8.7	CVE-2026-70882

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. While the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.5	CVE-2026-70885
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70886
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-70887
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. While the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.2	CVE-2026-70892
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via SQL to compromise Oracle Hyperion Data Relationship Management. While the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.2	CVE-2026-70893
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized update, insert or	2026-08-18	8.2	CVE-2026-70897

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	delete access to some of Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).			
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70899
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. While the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-70900
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70901
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Hyperion Data Relationship Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-70903
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Data Relationship Management executes to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70904
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in	2026-08-18	7.5	CVE-2026-70875

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Data Relationship Management executes to compromise Oracle Hyperion Data Relationship Management. While the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-70879
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70889
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70890
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70891
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Data Relationship Management executes to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.7	CVE-2026-70894
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70896
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized	2026-08-18	7.4	CVE-2026-70898

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Data Relationship Management executes to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Data Relationship Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.1	CVE-2026-70902
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 10.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	10	CVE-2026-70921
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70817
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-70854
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via SQL to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-70920
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via SQL to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70818
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with	2026-08-18	8.8	CVE-2026-70819

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Financial Management	network access via SQL to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via SQL to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70821
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 8.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.4	CVE-2026-70840
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 8.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.4	CVE-2026-70842
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	8.2	CVE-2026-70909
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via SQL to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70925
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via SQL to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and	2026-08-18	8.8	CVE-2026-70928

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70929
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70940
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70943
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70944
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	8.2	CVE-2026-70952
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71150
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible	2026-08-18	7.5	CVE-2026-70822

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-70823
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70828
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70832
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-70834
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7	CVE-2026-70914
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	7.1	CVE-2026-70933
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible	2026-08-18	7.1	CVE-2026-70934

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	7.1	CVE-2026-70935
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.1	CVE-2026-70936
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70937
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-70939
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70942
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70946
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion	2026-08-18	7.2	CVE-2026-70950

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Financial Management. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-70960
Oracle Corporation--Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-71117
Oracle Corporation--Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70739
Oracle Corporation--Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70740
Oracle Corporation--Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Reporting accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-70741
Oracle Corporation--Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70745
Oracle Corporation--Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70742

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	8.2	CVE-2026-70743
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-70744
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Reporting accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70746
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-70749
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70787
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-60391
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Reporting executes to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Reporting. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-70750
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 7.5	2026-08-18	7.5	CVE-2026-70752

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62457
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	9.6	CVE-2026-62463
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62539
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62541
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62543
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62544
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 9.6	2026-08-18	9.6	CVE-2026-70958

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-62471
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-62477
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-62485
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-62500
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-62501
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-62502
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in	2026-08-18	8.1	CVE-2026-62531

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	8.6	CVE-2026-62535
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70956
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70957
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	8.1	CVE-2026-70959
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.2	CVE-2026-70964
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70965
Oracle Corporation--Oracle Hyperion	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged	2026-08-18	8.8	CVE-2026-70966

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Infrastructure Technology	attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Lifecycle Management). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-60393
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-62467
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via SQL to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-62481
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-62492
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-62522
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.1	CVE-2026-62536

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.1	CVE-2026-62537
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-62538
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-62545
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-62550
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2026-08-18	7.3	CVE-2026-62551
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-62552
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion	2026-08-18	7.5	CVE-2026-62554

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-62581
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.1	CVE-2026-70967
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70971
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70973
Oracle Corporation-- Oracle Hyperion Profitability and Cost Management	Vulnerability in the Oracle Hyperion Profitability and Cost Management product of Oracle Hyperion (component: Deployment). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Profitability and Cost Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Profitability and Cost Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Profitability and Cost Management accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-70730
Oracle Corporation-- Oracle Hyperion Profitability and Cost Management	Vulnerability in the Oracle Hyperion Profitability and Cost Management product of Oracle Hyperion (component: Deployment). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Profitability and Cost Management. While the vulnerability is in Oracle Hyperion Profitability and Cost Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Profitability and Cost Management accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	8.6	CVE-2026-70721
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Profitability and Cost Management product of Oracle Hyperion (component: Deployment). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with	2026-08-18	8.1	CVE-2026-70738

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Profitability and Cost Management	network access via HTTP to compromise Oracle Hyperion Profitability and Cost Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Profitability and Cost Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Profitability and Cost Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Hyperion Profitability and Cost Management	Vulnerability in the Oracle Hyperion Profitability and Cost Management product of Oracle Hyperion (component: Deployment). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Profitability and Cost Management. While the vulnerability is in Oracle Hyperion Profitability and Cost Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Profitability and Cost Management accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70723
Oracle Corporation-- Oracle Hyperion Profitability and Cost Management	Vulnerability in the Oracle Hyperion Profitability and Cost Management product of Oracle Hyperion (component: Deployment). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Profitability and Cost Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Profitability and Cost Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Profitability and Cost Management. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	7.1	CVE-2026-70733
Oracle Corporation-- Oracle Hyperion Profitability and Cost Management	Vulnerability in the Oracle Hyperion Profitability and Cost Management product of Oracle Hyperion (component: Deployment). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Profitability and Cost Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Profitability and Cost Management. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-70735
Oracle Corporation-- Oracle Hyperion Profitability and Cost Management	Vulnerability in the Oracle Hyperion Profitability and Cost Management product of Oracle Hyperion (component: Deployment). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Profitability and Cost Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Profitability and Cost Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Profitability and Cost Management accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70736
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Identity Manager. While the vulnerability is in Oracle Identity Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-60720
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Identity Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60721
Oracle Corporation--	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker	2026-08-18	9.8	CVE-2026-60727

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Identity Manager	with network access via HTTP to compromise Oracle Identity Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via RMI to compromise Oracle Identity Manager. While the vulnerability is in Oracle Identity Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-61066
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Identity Manager. While the vulnerability is in Oracle Identity Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-60707
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Identity Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60715
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle Identity Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60716
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle Identity Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60722
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Identity Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61118
Oracle Corporation-- Oracle Identity Manager	Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: Installer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Identity Manager executes to compromise Oracle Identity Manager. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-71111
Oracle Corporation-- Oracle Identity	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via TLS to compromise Oracle Identity Manager	2026-08-18	9.9	CVE-2026-60990

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager Connector	Connector. While the vulnerability is in Oracle Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation--Oracle Identity Manager Connector	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via TLS to compromise Oracle Identity Manager Connector. While the vulnerability is in Oracle Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-60995
Oracle Corporation--Oracle Identity Manager Connector	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager Connector. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-60992
Oracle Corporation--Oracle Identity Manager Connector	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Connectors and Connector Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Identity Manager Connector. While the vulnerability is in Oracle Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-60996
Oracle Corporation--Oracle Identity Manager Connector	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Microsoft Active Directory). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Difficult to exploit vulnerability allows high privileged attacker with network access via LDAP to compromise Oracle Identity Manager Connector. While the vulnerability is in Oracle Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager Connector. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8	CVE-2026-60998
Oracle Corporation--Oracle Identity Manager Connector	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Identity Manager Connector executes to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager Connector. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-60991
Oracle Corporation--Oracle Identity Manager Connector	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Identity Manager Connector executes to compromise Oracle Identity Manager Connector. Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager Connector. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-60993
Oracle Corporation--Oracle Identity	Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Difficult to exploit vulnerability allows low privileged	2026-08-18	7.2	CVE-2026-60994

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Manager Connector	attacker with logon to the infrastructure where Oracle Identity Manager Connector executes to compromise Oracle Identity Manager Connector. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Identity Manager Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Identity Manager Connector accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Internet Directory	Vulnerability in the Oracle Internet Directory product of Oracle Fusion Middleware (component: OID LDAP Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Internet Directory. While the vulnerability is in Oracle Internet Directory, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Internet Directory. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	10	CVE-2026-61241
Oracle Corporation-- Oracle Internet Directory	Vulnerability in the Oracle Internet Directory product of Oracle Fusion Middleware (component: OID LDAP Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via LDAP to compromise Oracle Internet Directory. While the vulnerability is in Oracle Internet Directory, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Internet Directory. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-61248
Oracle Corporation-- Oracle Internet Directory	Vulnerability in the Oracle Internet Directory product of Oracle Fusion Middleware (component: OID LDAP Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Internet Directory. Successful attacks of this vulnerability can result in takeover of Oracle Internet Directory. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-61258
Oracle Corporation-- Oracle Internet Procurement Connector	Vulnerability in the Oracle Internet Procurement Connector product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Internet Procurement Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Internet Procurement Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Internet Procurement Connector accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70815
Oracle Corporation-- Oracle Internet Procurement Connector	Vulnerability in the Oracle Internet Procurement Connector product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Internet Procurement Connector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Internet Procurement Connector accessible data as well as unauthorized access to critical data or complete access to all Oracle Internet Procurement Connector accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-60759
Oracle Corporation-- Oracle iRecruitment	Vulnerability in the Oracle iRecruitment product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iRecruitment. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iRecruitment accessible data as well as unauthorized access to critical data or complete access to all Oracle iRecruitment accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70835

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle iSetup	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in takeover of Oracle iSetup. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70713
Oracle Corporation-- Oracle iSupplier Portal	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupplier Portal accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70777
Oracle Corporation-- Oracle iSupplier Portal	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle iSupplier Portal accessible data as well as unauthorized access to critical data or complete access to all Oracle iSupplier Portal accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-70779
Oracle Corporation-- Oracle Java SE	Vulnerability in Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 25.0.4 and 26.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-70906
Oracle Corporation-- Oracle Labor Distribution	Vulnerability in the Oracle Labor Distribution product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Labor Distribution. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Labor Distribution accessible data as well as unauthorized access to critical data or complete access to all Oracle Labor Distribution accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70782
Oracle Corporation-- Oracle Landed Cost Management	Vulnerability in the Oracle Landed Cost Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Landed Cost Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Landed Cost Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Landed Cost Management accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70833
Oracle Corporation-- Oracle Loans	Vulnerability in the Oracle Loans product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Loans. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Loans accessible data as well as unauthorized update, insert or delete access to some of Oracle Loans accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70844

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Loans	Vulnerability in the Oracle Loans product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Loans. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Loans accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Loans. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L).	2026-08-18	7.1	CVE-2026-70845
Oracle Corporation-- Oracle Managed File Transfer	Vulnerability in the Oracle Managed File Transfer product of Oracle Fusion Middleware (component: MFT Runtime Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle Managed File Transfer. While the vulnerability is in Oracle Managed File Transfer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Managed File Transfer. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-61003
Oracle Corporation-- Oracle Marketing	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Audience). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Marketing. While the vulnerability is in Oracle Marketing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70687
Oracle Corporation-- Oracle Marketing Encyclopedia System	Vulnerability in the Oracle Marketing Encyclopedia System product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Marketing Encyclopedia System. While the vulnerability is in Oracle Marketing Encyclopedia System, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing Encyclopedia System accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70692
Oracle Corporation-- Oracle MES for Process Manufacturing	Vulnerability in the Oracle MES for Process Manufacturing product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle MES for Process Manufacturing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle MES for Process Manufacturing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle MES for Process Manufacturing accessible data as well as unauthorized update, insert or delete access to some of Oracle MES for Process Manufacturing accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-61340
Oracle Corporation-- Oracle MES for Process Manufacturing	Vulnerability in the Oracle MES for Process Manufacturing product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle MES for Process Manufacturing. While the vulnerability is in Oracle MES for Process Manufacturing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle MES for Process Manufacturing accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70827
Oracle Corporation-- Oracle Operations Intelligence	Vulnerability in the Oracle Operations Intelligence product of Oracle E-Business Suite (component: Daily Business Intelligence). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Operations	2026-08-18	7.5	CVE-2026-70763

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Intelligence. Successful attacks of this vulnerability can result in takeover of Oracle Operations Intelligence. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation--Oracle Order Management	Vulnerability in the Oracle Order Management product of Oracle E-Business Suite (component: Product Diagnostic Tools). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Order Management. While the vulnerability is in Oracle Order Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Order Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Order Management accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70760
Oracle Corporation--Oracle Order Management	Vulnerability in the Oracle Order Management product of Oracle E-Business Suite (component: Product Diagnostic Tools). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Order Management. Successful attacks of this vulnerability can result in takeover of Oracle Order Management. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70930
Oracle Corporation--Oracle Order Management	Vulnerability in the Oracle Order Management product of Oracle E-Business Suite (component: Product Diagnostic Tools). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Order Management executes to compromise Oracle Order Management. While the vulnerability is in Oracle Order Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Order Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Order Management accessible data. CVSS 3.1 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	7.2	CVE-2026-70932
Oracle Corporation--Oracle Outside In Technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In PDF Export SDK). The supported version that is affected is 8.5.8. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Outside In Technology executes to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Outside In Technology. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-60392
Oracle Corporation--Oracle Outside In Technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Core). The supported version that is affected is 8.5.8. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Outside In Technology executes to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Outside In Technology. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-60412
Oracle Corporation--Oracle Outside In Technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Core). The supported version that is affected is 8.5.8. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Outside In Technology executes to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Outside In Technology. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-60413
Oracle Corporation--Oracle Outside In Technology	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Core). The supported version that is affected is 8.5.8. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Outside In Technology executes to compromise	2026-08-18	7.8	CVE-2026-60414

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Outside In Technology. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Partner Management	Vulnerability in the Oracle Partner Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Partner Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Partner Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Partner Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Partner Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-62605
Oracle Corporation-- Oracle Payables	Vulnerability in the Oracle Payables product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payables. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payables accessible data as well as unauthorized access to critical data or complete access to all Oracle Payables accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70701
Oracle Corporation-- Oracle Payables	Vulnerability in the Oracle Payables product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payables. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Payables. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-70700
Oracle Corporation-- Oracle Payments	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments. Successful attacks of this vulnerability can result in takeover of Oracle Payments. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60782
Oracle Corporation-- Oracle Payments	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Payments accessible data as well as unauthorized update, insert or delete access to some of Oracle Payments accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-70702
Oracle Corporation-- Oracle Payments	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payments. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Payments accessible data as well as unauthorized update, insert or delete access to some of Oracle Payments accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-60781
Oracle Corporation-- Oracle Payments	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Payments. While the vulnerability is in Oracle Payments, attacks may significantly impact additional products (scope	2026-08-18	7.7	CVE-2026-70694

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payments accessible data as well as unauthorized access to critical data or complete access to all Oracle Payments accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Payments	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Payments. While the vulnerability is in Oracle Payments, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payments accessible data as well as unauthorized access to critical data or complete access to all Oracle Payments accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	7.7	CVE-2026-70695
Oracle Corporation-- Oracle Payments	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Payments. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Payments accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70696
Oracle Corporation-- Oracle Payments	Vulnerability in the Oracle Payments product of Oracle E-Business Suite (component: File Transmission). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Payments. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payments accessible data as well as unauthorized access to critical data or complete access to all Oracle Payments accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-70699
Oracle Corporation-- Oracle Payroll	Vulnerability in the Oracle Payroll product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Payroll executes to compromise Oracle Payroll. While the vulnerability is in Oracle Payroll, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Payroll. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70941
Oracle Corporation-- Oracle Payroll	Vulnerability in the Oracle Payroll product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Payroll. While the vulnerability is in Oracle Payroll, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Payroll accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70945
Oracle Corporation-- Oracle Process Manufacturing Systems	Vulnerability in the Oracle Process Manufacturing Systems product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Systems. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Process Manufacturing Systems accessible data as well as unauthorized access to critical data or complete access to all Oracle Process Manufacturing Systems accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70830
Oracle Corporation-- Oracle Process Manufacturing Systems	Vulnerability in the Oracle Process Manufacturing Systems product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Systems. Successful attacks of this vulnerability can result in	2026-08-18	7.5	CVE-2026-70829

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	takeover of Oracle Process Manufacturing Systems. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Product Hub	Vulnerability in the Oracle Product Hub product of Oracle E-Business Suite (component: Outbound Data). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Product Hub. Successful attacks of this vulnerability can result in takeover of Oracle Product Hub. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70918
Oracle Corporation-- Oracle Product Lifecycle Analytics	Vulnerability in the Oracle Product Lifecycle Analytics product of Oracle Supply Chain (component: Installation Issues). The supported version that is affected is 3.6.1. Easily exploitable vulnerability allows low privileged attacker with network access via Oracle Net to compromise Oracle Product Lifecycle Analytics. While the vulnerability is in Oracle Product Lifecycle Analytics, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Product Lifecycle Analytics accessible data as well as unauthorized update, insert or delete access to some of Oracle Product Lifecycle Analytics accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	8.5	CVE-2026-71049
Oracle Corporation-- Oracle Product Lifecycle Analytics	Vulnerability in the Oracle Product Lifecycle Analytics product of Oracle Supply Chain (component: Installation Issues). The supported version that is affected is 3.6.1. Easily exploitable vulnerability allows high privileged attacker with network access via Oracle Net to compromise Oracle Product Lifecycle Analytics. While the vulnerability is in Oracle Product Lifecycle Analytics, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Product Lifecycle Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Product Lifecycle Analytics accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-71050
Oracle Corporation-- Oracle Product Lifecycle Analytics	Vulnerability in the Oracle Product Lifecycle Analytics product of Oracle Supply Chain (component: Installation Issues). The supported version that is affected is 3.6.1. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Product Lifecycle Analytics executes to compromise Oracle Product Lifecycle Analytics. While the vulnerability is in Oracle Product Lifecycle Analytics, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Product Lifecycle Analytics. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-71051
Oracle Corporation-- Oracle Product Lifecycle Analytics	Vulnerability in the Oracle Product Lifecycle Analytics product of Oracle Supply Chain (component: Installation Issues). The supported version that is affected is 3.6.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Product Lifecycle Analytics. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Product Lifecycle Analytics accessible data as well as unauthorized update, insert or delete access to some of Oracle Product Lifecycle Analytics accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Product Lifecycle Analytics. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	2026-08-18	7.6	CVE-2026-71048
Oracle Corporation-- Oracle Project Planning and Control	Vulnerability in the Oracle Project Planning and Control product of Oracle E-Business Suite (component: Change Management). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Planning and Control. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Project Planning and Control accessible data as well as unauthorized access to critical data or complete access to all Oracle Project Planning and Control accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70805

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Proposals	Vulnerability in the Oracle Proposals product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Proposals. Successful attacks of this vulnerability can result in takeover of Oracle Proposals. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-70781
Oracle Corporation-- Oracle Public Sector Human Resources	Vulnerability in the Oracle Public Sector Human Resources product of Oracle E-Business Suite (component: Regression Testing). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Public Sector Human Resources. While the vulnerability is in Oracle Public Sector Human Resources, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Public Sector Human Resources. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8	CVE-2026-70802
Oracle Corporation-- Oracle Public Sector Human Resources	Vulnerability in the Oracle Public Sector Human Resources product of Oracle E-Business Suite (component: Regression Testing). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Public Sector Human Resources. While the vulnerability is in Oracle Public Sector Human Resources, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Public Sector Human Resources accessible data as well as unauthorized access to critical data or complete access to all Oracle Public Sector Human Resources accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	7.7	CVE-2026-70804
Oracle Corporation-- Oracle Purchasing	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Purchasing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Purchasing accessible data as well as unauthorized access to critical data or complete access to all Oracle Purchasing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-62491
Oracle Corporation-- Oracle Purchasing	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.5-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Purchasing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Purchasing accessible data as well as unauthorized access to critical data or complete access to all Oracle Purchasing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70811
Oracle Corporation-- Oracle Purchasing	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Other issue). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Purchasing. Successful attacks of this vulnerability can result in takeover of Oracle Purchasing. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70948
Oracle Corporation-- Oracle Purchasing	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Purchasing. Successful attacks of this vulnerability can result in takeover of Oracle Purchasing. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-70797
Oracle Corporation-- Oracle Purchasing	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Purchasing executes to compromise Oracle	2026-08-18	7.8	CVE-2026-70798

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Purchasing. Successful attacks of this vulnerability can result in takeover of Oracle Purchasing. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Purchasing	Vulnerability in the Oracle Purchasing product of Oracle E-Business Suite (component: Other issue). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Purchasing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Purchasing accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70947
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows low privileged attacker with network access via CORBA to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-62608
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62609
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Reports Developer accessible data as well as unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-62610
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62611
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Reports Developer executes to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Reports Developer accessible data as well as unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	9.3	CVE-2026-62613
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62614
Oracle Corporation--	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with	2026-08-18	9.8	CVE-2026-62617

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Reports Developer	network access via UDP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data as well as unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	9.3	CVE-2026-62618
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62621
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOp to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62622
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOp to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62624
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62626
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Reports Developer accessible data as well as unauthorized read access to a subset of Oracle Reports Developer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Reports Developer. CVSS 3.1 Base Score 9.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H).	2026-08-18	9.4	CVE-2026-62629
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62630
Oracle Corporation--	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with	2026-08-18	9.8	CVE-2026-62632

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Reports Developer	network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62633
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via CORBA to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62634
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62635
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Reports Developer executes to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Reports Developer accessible data as well as unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	9.3	CVE-2026-62637
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Reports Developer accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Reports Developer. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	9.1	CVE-2026-62638
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via CORBA to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62639
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62640
Oracle Corporation--	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with	2026-08-18	9.1	CVE-2026-70668

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Reports Developer	network access via SOAP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Reports Developer accessible data as well as unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70669
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Reports Developer executes to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.6	CVE-2026-70670
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data as well as unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	9.3	CVE-2026-70673
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-62612
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.5	CVE-2026-62615
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:R/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-62619
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can	2026-08-18	8.6	CVE-2026-62620

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	result in unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Reports Developer executes to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-62623
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via SOAP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data as well as unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Reports Developer. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L).	2026-08-18	8.6	CVE-2026-62625
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	8.6	CVE-2026-62628
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Reports Developer executes to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-62631
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via SOAP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data as well as unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Reports Developer. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L).	2026-08-18	8.6	CVE-2026-62636
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Reports Developer accessible data as well as unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70671
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Reports Developer executes to compromise Oracle Reports Developer.	2026-08-18	8.8	CVE-2026-70674

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in takeover of Oracle Reports Developer. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-70675
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via SMTP to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Reports Developer. CVSS 3.1 Base Score 7.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L).	2026-08-18	7.2	CVE-2026-62616
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 12.2.1.19.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Reports Developer. While the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data as well as unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-62627
Oracle Corporation-- Oracle Reports Developer	Vulnerability in the Oracle Reports Developer product of Oracle Fusion Middleware (component: Security and Authentication). The supported version that is affected is 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Reports Developer accessible data as well as unauthorized access to critical data or complete access to all Oracle Reports Developer accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-70672
Oracle Corporation-- Oracle Risk Management	Vulnerability in the Oracle Risk Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Risk Management. Successful attacks of this vulnerability can result in takeover of Oracle Risk Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70761
Oracle Corporation-- Oracle Risk Management	Vulnerability in the Oracle Risk Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Risk Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Risk Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Risk Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70762
Oracle Corporation-- Oracle Sales	Vulnerability in the Oracle Sales product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sales. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sales accessible data as well as unauthorized access to critical data or complete access to all Oracle Sales accessible data. CVSS 3.1 Base Score 8.1	2026-08-18	8.1	CVE-2026-62600

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Sales	Vulnerability in the Oracle Sales product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sales. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Sales accessible data as well as unauthorized update, insert or delete access to some of Oracle Sales accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-62601
Oracle Corporation-- Oracle Sales	Vulnerability in the Oracle Sales product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sales. Successful attacks of this vulnerability can result in takeover of Oracle Sales. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70706
Oracle Corporation-- Oracle Sales for Handhelds	Vulnerability in the Oracle Sales for Handhelds product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sales for Handhelds. Successful attacks of this vulnerability can result in takeover of Oracle Sales for Handhelds. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70707
Oracle Corporation-- Oracle Sales Foundation	Vulnerability in the Oracle Sales Foundation product of Oracle E-Business Suite (component: Security API). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sales Foundation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sales Foundation accessible data as well as unauthorized access to critical data or complete access to all Oracle Sales Foundation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-70708
Oracle Corporation-- Oracle Sales Foundation	Vulnerability in the Oracle Sales Foundation product of Oracle E-Business Suite (component: Security API). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sales Foundation. Successful attacks of this vulnerability can result in takeover of Oracle Sales Foundation. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70710
Oracle Corporation-- Oracle Scripting	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks of this vulnerability can result in takeover of Oracle Scripting. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60976
Oracle Corporation-- Oracle Scripting	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Scripting accessible data as well as unauthorized update, insert or delete access to some of Oracle Scripting accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-70808
Oracle Corporation-- Oracle Scripting	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Scripting accessible data as well as unauthorized access to critical data or complete access to all Oracle Scripting accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle	2026-08-18	7.1	CVE-2026-70809

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Scripting. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:L).			
Oracle Corporation-- Oracle Scripting	Vulnerability in the Oracle Scripting product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Scripting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Scripting accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70810
Oracle Corporation-- Oracle SDP Number Portability	Vulnerability in the Oracle SDP Number Portability product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SDP Number Portability. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle SDP Number Portability accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70799
Oracle Corporation-- Oracle SDP Number Portability	Vulnerability in the Oracle SDP Number Portability product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle SDP Number Portability executes to compromise Oracle SDP Number Portability. While the vulnerability is in Oracle SDP Number Portability, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle SDP Number Portability accessible data as well as unauthorized read access to a subset of Oracle SDP Number Portability accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle SDP Number Portability. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:L).	2026-08-18	7.3	CVE-2026-70800
Oracle Corporation-- Oracle Service Contracts	Vulnerability in the Oracle Service Contracts product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Service Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Service Contracts accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-70783
Oracle Corporation-- Oracle Service Fulfillment Manager	Vulnerability in the Oracle Service Fulfillment Manager product of Oracle E-Business Suite (component: Fulfillment Engine). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Fulfillment Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Service Fulfillment Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Service Fulfillment Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Service Fulfillment Manager accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-70786
Oracle Corporation-- Oracle SOA Suite	Vulnerability in the Oracle SOA Suite product of Oracle Fusion Middleware (component: B2B Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in takeover of Oracle SOA Suite. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61002
Oracle Corporation-- Oracle Telecommunications Billing Integrator	Vulnerability in the Oracle Telecommunications Billing Integrator product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Telecommunications Billing Integrator. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Telecommunications	2026-08-18	7.4	CVE-2026-70790

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Billing Integrator, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Telecommunications Billing Integrator accessible data. CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N).			
Oracle Corporation-- Oracle Teleservice	Vulnerability in the Oracle Teleservice product of Oracle E-Business Suite (component: Service Request Form). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Teleservice. Successful attacks of this vulnerability can result in takeover of Oracle Teleservice. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70729
Oracle Corporation-- Oracle Trading Community	Vulnerability in the Oracle Trading Community product of Oracle E-Business Suite (component: Third Party Data Integration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trading Community. While the vulnerability is in Oracle Trading Community, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trading Community accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	8.6	CVE-2026-62599
Oracle Corporation-- Oracle Trading Community	Vulnerability in the Oracle Trading Community product of Oracle E-Business Suite (component: Party Search UI). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trading Community. Successful attacks of this vulnerability can result in takeover of Oracle Trading Community. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-70704
Oracle Corporation-- Oracle Transportation Execution	Vulnerability in the Oracle Transportation Execution product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Transportation Execution. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Transportation Execution, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Transportation Execution accessible data as well as unauthorized read access to a subset of Oracle Transportation Execution accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:I/H/A:N).	2026-08-18	7.6	CVE-2026-70791
Oracle Corporation-- Oracle U.S. Federal Financials	Vulnerability in the Oracle U.S. Federal Financials product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle U.S. Federal Financials. Successful attacks of this vulnerability can result in takeover of Oracle U.S. Federal Financials. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61319
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via LDAP to compromise Oracle Unified Directory. While the vulnerability is in Oracle Unified Directory, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Unified Directory. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.5	CVE-2026-60841
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via LDAP to compromise Oracle Unified Directory. While the vulnerability is in Oracle Unified Directory, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Unified Directory. CVSS 3.1 Base Score 8.5	2026-08-18	8.5	CVE-2026-60849

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Unified Directory accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-60850
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Unified Directory accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-60889
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Unified Directory accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-60914
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via LDAP to compromise Oracle Unified Directory. While the vulnerability is in Oracle Unified Directory, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Unified Directory accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-60969
Oracle Corporation-- Oracle Virtual Directory	Vulnerability in the Oracle Virtual Directory product of Oracle Fusion Middleware (component: Virtual Directory Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via LDAP to compromise Oracle Virtual Directory. Successful attacks of this vulnerability can result in takeover of Oracle Virtual Directory. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61231
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.2	CVE-2026-71129
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-71130
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM	2026-08-18	8.6	CVE-2026-71131

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via RDP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-71113
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-71116
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-71126
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	2026-08-18	7.3	CVE-2026-71136
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:H).	2026-08-18	7.3	CVE-2026-71138
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized	2026-08-18	7.7	CVE-2026-71141

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:L).			
Oracle Corporation--Oracle Warehouse Management	Vulnerability in the Oracle Warehouse Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Warehouse Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Warehouse Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Warehouse Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Warehouse Management. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L).	2026-08-18	8.3	CVE-2026-70770
Oracle Corporation--Oracle Warehouse Management	Vulnerability in the Oracle Warehouse Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Warehouse Management. While the vulnerability is in Oracle Warehouse Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Warehouse Management accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-70771
Oracle Corporation--Oracle Warehouse Management	Vulnerability in the Oracle Warehouse Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Warehouse Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Warehouse Management accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70772
Oracle Corporation--Oracle Warehouse Management	Vulnerability in the Oracle Warehouse Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Warehouse Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Warehouse Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Warehouse Management. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L).	2026-08-18	7.1	CVE-2026-70774
Oracle Corporation--Oracle Web Services Manager	Vulnerability in the Oracle Web Services Manager product of Oracle Fusion Middleware (component: Web Services Security). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Services Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Services Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Services Manager accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-60737
Oracle Corporation--Oracle Web Services Manager	Vulnerability in the Oracle Web Services Manager product of Oracle Fusion Middleware (component: Web Services Security). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Web Services Manager. While the vulnerability is in Oracle Web Services Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Web Services Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Web Services Manager accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	9.6	CVE-2026-61001

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Web Services Manager	Vulnerability in the Oracle Web Services Manager product of Oracle Fusion Middleware (component: Web Services Security). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Web Services Manager. Successful attacks of this vulnerability can result in takeover of Oracle Web Services Manager. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-70924
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Content. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L).	2026-08-18	9.6	CVE-2026-60905
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-60903
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle WebCenter Content executes to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.4	CVE-2026-60928
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-60934
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle	2026-08-18	8.7	CVE-2026-60935

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-60944
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-60954
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Content. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:L).	2026-08-18	8.2	CVE-2026-60955
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle WebCenter Content executes to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8	CVE-2026-60961
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-60980
Oracle Corporation--	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 14.1.2.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged	2026-08-18	8.7	CVE-2026-60981

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle WebCenter Content	attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-60906
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	7.6	CVE-2026-60909
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-60933
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-60949
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 14.1.2.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-60983
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person	2026-08-18	7.1	CVE-2026-61288

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).			
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.1	CVE-2026-61290
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle WebCenter Content executes to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-61291
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle WebCenter Content executes to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.1	CVE-2026-61295
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data as well as unauthorized read access to a subset of Oracle WebCenter Content accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Content. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L).	2026-08-18	7.1	CVE-2026-70858
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Enterprise Capture accessible data as well as unauthorized read access to a subset of Oracle WebCenter Enterprise Capture accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:L).	2026-08-18	9.9	CVE-2026-60916
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. Successful attacks of this vulnerability can result in takeover of	2026-08-18	9.8	CVE-2026-60921

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle WebCenter Enterprise Capture. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60946
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle WebCenter Enterprise Capture. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60947
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Enterprise Capture. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60958
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60970
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60971
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Portlet Services). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H).	2026-08-18	9.1	CVE-2026-60728
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-60730
Oracle Corporation--	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker	2026-08-18	9.8	CVE-2026-70970

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle WebCenter Portal	with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60729
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via RMI to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60731
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-61177
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-61193
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.5	CVE-2026-61212
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61213
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data.	2026-08-18	8.7	CVE-2026-61215

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-61219
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-61222
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	8.6	CVE-2026-61228
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-61229
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	8.6	CVE-2026-61230
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data as well as unauthorized read access to a subset of Oracle WebCenter Portal accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Portal. CVSS 3.1 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:L).	2026-08-18	7.7	CVE-2026-60733

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Portal accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Portal. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:L).	2026-08-18	7.1	CVE-2026-61124
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/H/I:N/A:N).	2026-08-18	7.7	CVE-2026-61199
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Portal accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Portal. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	2026-08-18	7.6	CVE-2026-61208
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Portal accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/H/I:L/A:N).	2026-08-18	7.6	CVE-2026-61227
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Sites accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	9.1	CVE-2026-61008
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-61018
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can	2026-08-18	9.9	CVE-2026-61021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9	CVE-2026-61029
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.1	CVE-2026-61034
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Sites accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L).	2026-08-18	8.2	CVE-2026-61011
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Sites accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L).	2026-08-18	8.2	CVE-2026-61016
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61017
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61022
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61032
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful	2026-08-18	8.6	CVE-2026-61033

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L).			
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-61038
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61040
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61042
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L).	2026-08-18	8.6	CVE-2026-61045
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	8.2	CVE-2026-61054
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61058
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score	2026-08-18	7.5	CVE-2026-61007

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).			
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60672
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60696
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60698
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-60702
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60977
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-60415
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	8.1	CVE-2026-60680
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle	2026-08-18	8.6	CVE-2026-60699

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WebLogic Server accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).			
Oracle Corporation-- Oracle WebLogic Server	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-60679
Oracle Corporation-- Oracle Work in Process	Vulnerability in the Oracle Work in Process product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in takeover of Oracle Work in Process. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-62462
Oracle Corporation-- Oracle Work in Process	Vulnerability in the Oracle Work in Process product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Work in Process executes to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in takeover of Oracle Work in Process. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7	CVE-2026-62449
Oracle Corporation-- Oracle Work in Process	Vulnerability in the Oracle Work in Process product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Work in Process as well as unauthorized update, insert or delete access to some of Oracle Work in Process accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).	2026-08-18	7.1	CVE-2026-62458
Oracle Corporation-- Oracle Workflow	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Notification Mailer). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via SMTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in takeover of Oracle Workflow. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-70926
Oracle Corporation-- Oracle Workflow	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Notification Mailer). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Workflow accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Workflow. CVSS 3.1 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	8.1	CVE-2026-70931
Oracle Corporation-- Oracle Workflow	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Workflow Notification Mailer). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Workflow. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	7.5	CVE-2026-70927
Oracle Corporation-- Oracle Yard Management	Vulnerability in the Oracle Yard Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Yard Management. Successful attacks of this vulnerability can result in takeover of Oracle Yard Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70792

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- PeopleSoft Enterprise CC Common Application Objects	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects product of Oracle PeopleSoft (component: Common Application Objects). The supported version that is affected is 9.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise PeopleSoft Enterprise CC Common Application Objects. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise CC Common Application Objects. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-61307
Oracle Corporation-- PeopleSoft Enterprise FIN Common Objects	Vulnerability in the PeopleSoft Enterprise FIN Common Objects product of Oracle PeopleSoft (component: Security). The supported version that is affected is 9.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Common Objects. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise FIN Common Objects. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-71112
Oracle Corporation-- PeopleSoft Enterprise FIN Common Objects Brazil	Vulnerability in the PeopleSoft Enterprise FIN Common Objects Brazil product of Oracle PeopleSoft (component: Common Objects). The supported version that is affected is 9.1. Easily exploitable vulnerability allows high privileged attacker with network access via T3, IIOP to compromise PeopleSoft Enterprise FIN Common Objects Brazil. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise FIN Common Objects Brazil. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-70861
Oracle Corporation-- PeopleSoft Enterprise FIN Lease Administration	Vulnerability in the PeopleSoft Enterprise FIN Lease Administration product of Oracle PeopleSoft (component: Lease Administration). The supported version that is affected is 9.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where PeopleSoft Enterprise FIN Lease Administration executes to compromise PeopleSoft Enterprise FIN Lease Administration. While the vulnerability is in PeopleSoft Enterprise FIN Lease Administration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise FIN Lease Administration accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise FIN Lease Administration accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	7.5	CVE-2026-71092
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Business Interlink). Supported versions that are affected are 8.61-8.63. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-60821
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.61-8.63. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-60742
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Integration Broker). Supported versions that are affected are 8.61-8.63. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.1	CVE-2026-60831
Oracle Corporation--	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Configuration Manager). Supported versions that are	2026-08-18	8.8	CVE-2026-60879

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PeopleSoft Enterprise PeopleTools	affected are 8.61-8.63. Easily exploitable vulnerability allows low privileged attacker with network access via SQL to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: nVision). Supported versions that are affected are 8.61-8.63. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60967
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Install and Packaging). Supported versions that are affected are 8.61-8.63. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-60856
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Data Mover). Supported versions that are affected are 8.61-8.63. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:L).	2026-08-18	7.2	CVE-2026-60873
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PeopleCode). Supported versions that are affected are 8.61-8.63. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.2	CVE-2026-60883
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Tuxedo). Supported versions that are affected are 8.61-8.63. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7	CVE-2026-60902
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.61 and 8.62. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PeopleTools executes to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all	2026-08-18	7.5	CVE-2026-60975

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Service Delivery Platform	Vulnerability in the Service Delivery Platform product of Oracle Fusion Middleware (component: Messaging Enabler). Supported versions that are affected are 14.1.2.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via Oracle Net to compromise Service Delivery Platform. While the vulnerability is in Service Delivery Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Service Delivery Platform accessible data as well as unauthorized access to critical data or complete access to all Service Delivery Platform accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	9.6	CVE-2026-60861
Oracle Corporation-- Service Delivery Platform	Vulnerability in the Service Delivery Platform product of Oracle Fusion Middleware (component: Messaging Enabler). Supported versions that are affected are 14.1.2.0.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TCP to compromise Service Delivery Platform. While the vulnerability is in Service Delivery Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Service Delivery Platform accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Service Delivery Platform. CVSS 3.1 Base Score 8.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H).	2026-08-18	8.7	CVE-2026-60860
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel Apps - Marketing accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H).	2026-08-18	9.1	CVE-2026-60754
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60751
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-60767
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel Apps - Marketing accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Siebel Apps - Marketing. CVSS 3.1 Base Score 8.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H).	2026-08-18	8.1	CVE-2026-60779
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel Apps - Marketing accessible data and unauthorized ability to cause a	2026-08-18	7.1	CVE-2026-60752

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	partial denial of service (partial DOS) of Siebel Apps - Marketing. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).			
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-60765
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel Apps - Marketing accessible data as well as unauthorized access to critical data or complete access to all Siebel Apps - Marketing accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-60803
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Email Marketing). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Siebel Apps - Marketing executes to compromise Siebel Apps - Marketing. While the vulnerability is in Siebel Apps - Marketing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel Apps - Marketing accessible data as well as unauthorized access to critical data or complete access to all Siebel Apps - Marketing accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	7.5	CVE-2026-60808
Oracle Corporation-- Siebel Apps - Self Service	Vulnerability in the Siebel Apps - Self Service product of Oracle Siebel CRM (component: Helpdesk/Training). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Self Service. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel Apps - Self Service, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel Apps - Self Service accessible data as well as unauthorized access to critical data or complete access to all Siebel Apps - Self Service accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).	2026-08-18	9.3	CVE-2026-70855
Oracle Corporation-- Siebel Artificial Intelligence	Vulnerability in the Siebel Artificial Intelligence product of Oracle Siebel CRM (component: AI). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Artificial Intelligence. While the vulnerability is in Siebel Artificial Intelligence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel Artificial Intelligence accessible data as well as unauthorized update, insert or delete access to some of Siebel Artificial Intelligence accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	8.5	CVE-2026-60758
Oracle Corporation-- Siebel CRM Administration	Vulnerability in the Siebel CRM Administration product of Oracle Siebel CRM (component: Data Archival). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Administration. Successful attacks of this vulnerability can result in takeover of Siebel CRM Administration. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62585
Oracle Corporation-- Siebel CRM Administration	Vulnerability in the Siebel CRM Administration product of Oracle Siebel CRM (component: Data Archival). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Administration. While the vulnerability	2026-08-18	8.6	CVE-2026-62586

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is in Siebel CRM Administration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Administration accessible data. CVSS 3.1 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).			
Oracle Corporation-- Siebel CRM Administration	Vulnerability in the Siebel CRM Administration product of Oracle Siebel CRM (component: Data Archival). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Administration. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Administration accessible data as well as unauthorized update, insert or delete access to some of Siebel CRM Administration accessible data. CVSS 3.1 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	7.1	CVE-2026-62587
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-61317
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-61318
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Cloud Applications accessible data as well as unauthorized update, insert or delete access to some of Siebel CRM Cloud Applications accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L).	2026-08-18	9.9	CVE-2026-62452
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-62512
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Cloud Applications accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Cloud Applications accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-61321
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. While the	2026-08-18	8.5	CVE-2026-61326

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Cloud Applications accessible data as well as unauthorized update, insert or delete access to some of Siebel CRM Cloud Applications accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).			
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61330
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Cloud Applications accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Cloud Applications accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-61332
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-61341
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Siebel CRM Cloud Applications executes to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Cloud Applications accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Cloud Applications accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-62442
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Cloud Applications accessible data as well as unauthorized read access to a subset of Siebel CRM Cloud Applications accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H).	2026-08-18	8.3	CVE-2026-62455
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Siebel CRM Cloud Applications executes to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Cloud Applications accessible data as well as unauthorized update, insert or delete access to some of Siebel CRM Cloud	2026-08-18	7.3	CVE-2026-61339

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Applications accessible data. CVSS 3.1 Base Score 7.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).			
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 22.3-26.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Siebel CRM Cloud Applications executes to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-62454
Oracle Corporation-- Siebel CRM Deployment	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Application Interface). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Siebel CRM Deployment executes to compromise Siebel CRM Deployment. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Deployment accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Deployment accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-60791
Oracle Corporation-- Siebel CRM Deployment	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Migration). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Deployment. While the vulnerability is in Siebel CRM Deployment, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Deployment accessible data as well as unauthorized update, insert or delete access to some of Siebel CRM Deployment accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	8.5	CVE-2026-60798
Oracle Corporation-- Siebel CRM Deployment	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Server Infrastructure). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Deployment. Successful attacks of this vulnerability can result in takeover of Siebel CRM Deployment. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70949
Oracle Corporation-- Siebel CRM Deployment	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Installation). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Siebel CRM Deployment executes to compromise Siebel CRM Deployment. Successful attacks of this vulnerability can result in takeover of Siebel CRM Deployment. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	7.8	CVE-2026-60753
Oracle Corporation-- Siebel CRM Deployment	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Server Infrastructure). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Deployment. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Deployment accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Deployment accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-60792
Oracle Corporation-- Siebel CRM Deployment	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Migration). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Deployment. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Siebel CRM Deployment. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	7.5	CVE-2026-70856
Oracle Corporation--	Vulnerability in the Siebel CRM End User product of Oracle Siebel CRM (component: Search). Supported versions that are affected are 17.0-26.6. Easily	2026-08-18	8.1	CVE-2026-60757

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siebel CRM End User	exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Siebel CRM End User executes to compromise Siebel CRM End User. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM End User accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM End User accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Siebel CRM End User	Vulnerability in the Siebel CRM End User product of Oracle Siebel CRM (component: Document Management). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM End User. Successful attacks of this vulnerability can result in takeover of Siebel CRM End User. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	8.8	CVE-2026-70951
Oracle Corporation-- Siebel CRM End User	Vulnerability in the Siebel CRM End User product of Oracle Siebel CRM (component: Open UI). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTPS to compromise Siebel CRM End User. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel CRM End User, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM End User accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM End User accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:N).	2026-08-18	7.7	CVE-2026-70857
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Integration. While the vulnerability is in Siebel CRM Integration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Integration. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	9.9	CVE-2026-62588
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in takeover of Siebel CRM Integration. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	9.8	CVE-2026-62592
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: REST). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Siebel CRM Integration. CVSS 3.1 Base Score 8.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L).	2026-08-18	8.2	CVE-2026-60796
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-26.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Integration. While the vulnerability is in Siebel CRM Integration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Integration accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-08-18	8.7	CVE-2026-62589
Oracle Corporation--	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-	2026-08-18	8.5	CVE-2026-62590

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siebel CRM Integration	26.6. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Integration. While the vulnerability is in Siebel CRM Integration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Integration. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Integration. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Integration accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-62591
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Siebel CRM Integration executes to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Integration accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	8.1	CVE-2026-62595
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Integration. While the vulnerability is in Siebel CRM Integration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data as well as unauthorized update, insert or delete access to some of Siebel CRM Integration accessible data. CVSS 3.1 Base Score 8.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	8.5	CVE-2026-62596
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: REST). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Integration. While the vulnerability is in Siebel CRM Integration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Integration. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-08-18	8.5	CVE-2026-70859
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: REST). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Integration accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-60766
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: REST). Supported versions that are affected are 17.0-26.6. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Integration accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	7.4	CVE-2026-60797
Oracle Corporation--	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: REST). Supported versions that are affected are 17.0-26.6. Difficult to	2026-08-18	7.4	CVE-2026-60820

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siebel CRM Integration	exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Integration accessible data as well as unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation--Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-26.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Integration. While the vulnerability is in Siebel CRM Integration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data. CVSS 3.1 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	7.7	CVE-2026-62593
Oracle Corporation--Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: Open Integration). Supported versions that are affected are 25.12-26.6. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Siebel CRM Integration. While the vulnerability is in Siebel CRM Integration, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Siebel CRM Integration accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Siebel CRM Integration. CVSS 3.1 Base Score 7.7 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:H/A:H).	2026-08-18	7.7	CVE-2026-62594
Oracle Corporation--Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: REST). Supported versions that are affected are 17.0-26.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel CRM Integration accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	7.5	CVE-2026-70910
orval-labs--orval	Orval generates type-safe JavaScript clients in TypeScript from OpenAPI v3 and Swagger v2 specifications. Prior to 8.22.0, Orval resolves remote and local external \$ref values without an allowlist or confinement to the input directory. Processing an attacker-controlled OpenAPI description can cause requests from the developer or CI host to attacker-selected or internal HTTP services, read absolute or out-of-tree local files, and inline untrusted remote schemas into generated clients. The affected code is packages/orval/src/import-specs.ts external reference loading. This issue is fixed in version 8.22.0.	2026-08-19	7.1	CVE-2026-62680
oscal-compass--compliance-trestle	compliance-trestle is a tooling platform for managing compliance as code. Prior to versions 3.12.2 and 4.0.3, the '-o/--output' argument in 'trestle author jinja' allows writing files outside the intended workspace. The application does not properly validate, '..', '..', or absolute paths. This allows arbitrary file write to attacker-controlled locations. Versions 3.12.3 and 4.0.3 patch the issue.	2026-08-17	8.4	CVE-2026-46345
Otalio--Ship Property Management System	Missing signature validation in JSON Web Tokens in Otalio Ship Property Management System versions before 2.22.0 allows authenticated attackers to escalate privileges via tampering with JWTs	2026-08-18	8.1	CVE-2025-9210
Outanking Team--Outranking Plugin Options	Unauthenticated Broken Access Control in Outranking Plugin Options <= 1.1.3 versions.	2026-08-19	7.5	CVE-2026-73385
Ozols Grupa--OZOLS	Download of code without integrity check, inclusion of functionality from untrusted control sphere, and cleartext transmission of sensitive information vulnerability in Ozols Grupa OZOLS on Windows caused by an abandoned auto-update domain. Affected component: the automatic update channel - OzolsSQL client update path, the <db>_update SQL Server Agent job (@subsystem = N'ActiveScripting') and serv_update.vbs. This issue affects OZOLS: before 1.1.1233.	2026-08-19	10	CVE-2026-22306
Paolo--GeoDirectory	Unauthenticated Cross Site Scripting (XSS) in GeoDirectory <= 2.8.173 versions.	2026-08-20	7.1	CVE-2026-66604

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
paperclipai--paperclip	Paperclip before 0.3.1 in default local_trusted mode fails to validate Host headers, allowing attackers to execute arbitrary commands via DNS rebinding. An attacker can craft a malicious webpage that, when visited by a developer running Paperclip locally, uses DNS rebinding to make authenticated API requests and execute commands through the process adapter.	2026-08-21	9.6	CVE-2026-77087
patrickhener--goshs	goshs is a SimpleHTTPServer written in Go. Prior to version 2.1.0, when `goshs` is launched with WebDAV enabled (`-w`), the mode-restriction flags `--read-only`, `--upload-only`, and `--no-delete` are enforced only on the primary HTTP port. The WebDAV port is wired straight to `golang.org/x/net/webdav.Handler` with no equivalent guard, so an authenticated WebDAV client can `PUT`, `DELETE`, `MKCOL`, `MOVE`, and `COPY` despite the operator's stated intent. Version 2.1.0 patches the issue.	2026-08-18	8.1	CVE-2026-50138
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.6, handleException() in lib/setup-sandbox.js sanitizes SuppressedError.error, SuppressedError.suppressed, and AggregateError.errors but does not sanitize Error.cause, allowing sandbox code to obtain a powerful host object such as process from an embedder-exposed host function that throws an error with that object as its cause and then execute arbitrary host commands. This issue is fixed in version 3.11.6.	2026-08-17	9.9	CVE-2026-47686
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to 3.11.6, lib/bridge.js and lib/setup-sandbox.js fail to block stacked indirection through Function.prototype.call around dangerous host prototype getter and setter mutators, allowing sandbox code to sever a host intrinsic's prototype chain and reach e.constructor.constructor for arbitrary host command execution. This issue is fixed in version 3.11.6.	2026-08-17	9.8	CVE-2026-47698
paulepro2019--EPROLO Dropshipping	Unauthenticated Broken Access Control in EPROLO Dropshipping <= 2.4.2 versions.	2026-08-20	7.1	CVE-2026-74019
Paymob--Paymob for WooCommerce	Unauthenticated Cross Site Scripting (XSS) in Paymob for WooCommerce <= 4.1.10 versions.	2026-08-20	7.1	CVE-2026-66611
PeepSo--Community by PeepSo	Subscriber SQL Injection in Community by PeepSo <= 9.0.5.2 versions.	2026-08-19	8.5	CVE-2026-66668
perber--leafwiki	LeafWiki is a self-hosted wiki. Versions 0.1.0 through 0.10.0 have a privilege escalation vulnerability in the user update API. An authenticated user could update their own account role and escalate privileges from a regular user, such as `viewer`, to `admin`. Exploitation requires a valid authenticated LeafWiki user account. Instances without public registration and with only trusted users are at lower practical risk. Users should update to version 0.10.1 or greater. Until a patch is available, operators should restrict account creation and ensure that only trusted users have accounts on affected LeafWiki instances. If possible, access to the user update API should be restricted to trusted users or administrators only.	2026-08-21	8.8	CVE-2026-53527
perber--leafwiki	LeafWiki is a self-hosted wiki. Versions 0.3.0 through 0.10.0 have a path traversal vulnerability in LeafWiki's asset rename functionality. An authenticated user with editor permissions could move files that are accessible to the LeafWiki server process into a page's asset directory. This could allow sensitive local files, such as the application database, to become downloadable as page assets. Users should update to version 0.10.1 or greater. As an additional mitigation, operators should ensure that the LeafWiki process runs with the least privileges necessary and does not have filesystem access to sensitive files outside the application's required directories. Until a patch is applied, operators may reduce risk by restricting editor access to trusted users only and by limiting the filesystem permissions of the LeafWiki process.	2026-08-21	8.8	CVE-2026-53528
PHPGurukul--Complaint Management System	A weakness has been identified in PHPGurukul Complaint Management System 1.0. Affected by this issue is some unknown functionality of the file user/check_availability.php. This manipulation of the argument email causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	2026-08-18	7.3	CVE-2026-75089
phpipam--phpipam	phpIPAM through 1.8.1 fails to verify that a requested IP address belongs to the subnet a temporary share token was issued for. In app/temp_share/index.php and app/temp_share/address.php, when the share type is 'subnets', the subnetId parameter is used directly as a database primary key to fetch an address without confirming the address belongs to the authorized subnet. An unauthenticated party holding any valid, non-expired temporary share URL can enumerate the	2026-08-17	7.5	CVE-2026-75105

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	subnetId parameter to read every IP address record across all sections and subnets, including hostnames, DNS names, MAC addresses, owner/contact fields, and notes (which may contain credentials and configuration details).			
Piotnet--Piotnet Addons For Elementor Pro	Unauthenticated Arbitrary File Upload in Piotnet Addons For Elementor Pro <= 7.1.67 versions.	2026-08-18	9.6	CVE-2026-28192
plainware--Locatoraid Store Locator	Unauthenticated SQL Injection in Locatoraid Store Locator <= 3.9.72 versions.	2026-08-20	9.3	CVE-2026-66680
postcss--postcss	PostCSS takes a CSS file and provides an API to analyze and modify its rules by transforming the rules into an Abstract Syntax Tree. Prior to 8.5.18, lib/previous-map.js loadMap() passes attacker-controlled sourceMappingURL values to join(dirname(opts.from), annotation), and loadFile() permits traversed or absolute .map paths, allowing untrusted CSS processed without map: false to disclose sourcesContent from arbitrary reachable .map files through result.map. This issue is fixed in version 8.5.18.	2026-08-17	7.5	CVE-2026-73646
Premio--Chaty Pro	Unauthenticated Cross Site Scripting (XSS) in Chaty Pro <= 3.5.8 versions.	2026-08-18	7.1	CVE-2026-73360
ProfessionalWiki--Maps	Maps is a MediaWiki extension that enables visualization of geographic data through dynamic embedded maps. Prior to version 12.1.3, the display_map parser function in the Leaflet service accepts attacker-controlled HTML in the overlays parameter, and resources/leaflet/jquery.leaflet.js uses the overlay name as a Leaflet layer-control label without escaping it. A wiki user with the edit permission can store malicious wikitext that causes script execution when another user previews or views the affected map. The script executes in the viewing user's browser session and can access data or perform actions available to that user. This issue is fixed in version 12.1.3.	2026-08-18	8.6	CVE-2026-52854
Progress--ShareFile Storage Zones Controller	In Progress ShareFile Storage Zones Controller v5.12.5 and below versions, unsafe deserialization of untrusted file metadata can allow a user with write access to a Network share to execute arbitrary code on the Storage Zones Controller host.	2026-08-17	8	CVE-2026-16138
Progress--ShareFile Storage Zones Controller	In Progress ShareFile Storage Zones Controller v5.12.5 and below, a party with valid zone credentials can perform path traversal using resumable upload initiation endpoint, allowing the party to write arbitrary content to any location writable by the application's service account. This may result in the execution of attacker-supplied code.	2026-08-17	7.2	CVE-2026-16137
Progress--ShareFile Storage Zones Controller	In Progress ShareFile Storage Zones Controller versions <= 5.12.5 and <= 6.0.2, an authenticated zone administrator can exploit improper validation in the download preparation flow, enabling attacker-controlled files to be written outside the intended preparation directory. This can lead to remote code execution in v5 versions. Remote code execution is not confirmed on v6 versions.	2026-08-17	7.2	CVE-2026-16139
PSM Plugins--SupportCandy	Unauthenticated Broken Authentication in SupportCandy <= 3.5.1 versions.	2026-08-18	8.2	CVE-2026-73350
QuantumNous--new-api	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to 1.0.0-rc.7, the admin user list and user lookup APIs, including GET /api/user/, return User.AccessToken as access_token because User model objects are serialized after queries use Omit("password"), allowing an authenticated administrator to obtain the root user's bearer token and access root-only system configuration APIs. This issue is fixed in version 1.0.0-rc.7.	2026-08-17	9.1	CVE-2026-64859
QuantumNous--new-api	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to 1.0.0-rc.18, user-controlled image n, video seconds and duration, max_tokens, max_completion_tokens, maxOutputTokens, audio duration, and billing-expression quantities can overflow conversions in common/quota_math.go and related settlement paths, allowing a low-privileged account with positive balance or an active subscription to turn a negative charge into account credit and potentially drain upstream funds. This issue is fixed in version 1.0.0-rc.18.	2026-08-17	9.1	CVE-2026-71479
QuantumNous--new-api	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to 1.0.0-rc.11, POST /api/stripe/webhook, POST /api/creem/webhook, and POST /api/waffo/webhook read and log full request bodies before signature validation in router/api-router.go and the payment controllers, allowing an unauthenticated attacker to cause memory pressure, container restarts, or disk exhaustion without forging a successful payment. This issue is fixed in version 1.0.0-rc.11.	2026-08-17	7.5	CVE-2026-64868
Rapid7--Velociraptor	Velociraptor's web GUI allows specifying a custom type for columns in tables. The URL type takes the cell value and forms a URL which can be clicked in the GUI.The	2026-08-18	8.1	CVE-2026-15371

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	code does not limit the schemes allowed in this URL , allowing an attacker to specify a JavaScript scheme exposing the user to XSS.			
RARgames--4gaBoards	4gaBoards is a boards system for realtime project management. Prior to 3.3.8, 4gaBoards allows an authenticated project manager to supply traversal sequences in the filename parameter of GET /exports/:id/:filename. In server/api/controllers/boards/download.js, the decoded inputs.filename value is passed to path.join() beneath private/exports/<user_id>/ without containment validation. A crafted value such as ../ can select an arbitrary file readable by the server process, and the file is returned to the attacker. The fileStream close handler then passes the same path to fs.unlink(), deleting the selected file and potentially causing data loss or denial of service. This issue is fixed in version 3.3.8.	2026-08-18	8.8	CVE-2026-50186
RARgames--4gaBoards	4gaBoards is a boards system for realtime project management. Prior to 3.3.8, 4gaBoards is vulnerable to pre-account takeover when registrationEnabled, localRegistrationEnabled, and ssoRegistrationEnabled are enabled and Google, GitHub, Microsoft, or OIDC SSO is configured. The POST /api/register endpoint permits creation of an unverified local account with a victim's email address, and POST /api/access-tokens permits that account to authenticate while isVerified is false. During the victim's first SSO login, server/api/helpers/users/get-create-one-for-github-sso.js, server/api/helpers/users/get-create-one-for-google-sso.js, server/api/helpers/users/get-create-one-for-microsoft-sso.js, and server/api/helpers/users/get-create-one-for-oidc-sso.js find the attacker-controlled account by email and link the verified SSO identity without confirming ownership of the local account. The attacker can retain local-password access to the linked account and obtain the victim's projects, data, and permissions. This issue is fixed in version 3.3.8.	2026-08-18	8.8	CVE-2026-50191
RARgames--4gaBoards	4gaBoards is a boards system for realtime project management. Prior to 3.3.9, 4gaBoards allows an authenticated user to modify ssoGoogleId, ssoGoogleEmail, ssoGithubId, ssoGithubUsername, ssoGithubEmail, ssoMicrosoftId, ssoMicrosoftEmail, ssoOidcId, and ssoOidcEmail through PATCH /api/users/:id. The whitelist in server/api/controllers/users/update.js mass assigns these backend-managed identity attributes from user input. An attacker can place a victim's provider identifier on an attacker-controlled account, causing the default lookup in helpers such as server/api/helpers/users/get-create-one-for-github-sso.js to match the victim's first SSO login to the attacker's account before the email-linkage flow runs. The victim is logged into the attacker-controlled account, and projects, boards, or data the victim creates remain accessible through the attacker's original local credentials. This issue is fixed in version 3.3.9.	2026-08-18	7.6	CVE-2026-53958
rayhanduitku--Duitku Payment Gateway	Unauthenticated Sensitive Data Exposure in Duitku Payment Gateway <= 2.11.14 versions.	2026-08-18	7.5	CVE-2026-32468
reconmap--reconmap	Reconmap's API applies a fallback authorization policy in apps/api/app/Program.cs that requires an authenticated user holding the administrator role, so controllers without their own attribute reject anonymous callers. The report preview action in apps/api/app/Controllers/ReportsController.cs carries [AllowAnonymous] and therefore opts out of that policy. PreviewReport loads the Project row named by the id path segment, loads the linked Organisation through the project's ClientId, and renders both into default-report-template.html, which prints the project name and description together with the client organisation's name, address and URL. No authentication, project membership or role check is performed. Because the id is the auto-increment primary key of the project table, an unauthenticated remote caller can walk sequential ids to retrieve the engagement details and client organisation of every project on the instance, and the 404 returned for a missing id reveals which project ids exist. Reconmap stores penetration-testing engagements, so the disclosed descriptions and client records are sensitive by nature.	2026-08-21	7.5	CVE-2026-77767
Red Hat--Migration Toolkit for Containers	In binutils 2.46.1 and prior versions, a victim who opens a crafted PE file using binutils could execute arbitrary code unknowingly via a stack buffer overflow out of bounds write.	2026-08-20	7.8	CVE-2026-19582
Red Hat--Multicluster Engine for Kubernetes	A flaw was found in the `cluster-proxy-addon` component of Multicluster Engine for Kubernetes. This vulnerability allows an unauthenticated attacker, who can access the user-facing route, to bypass authentication and authorization checks. By manipulating URL path segments, the attacker can proxy requests to arbitrary services across any managed cluster. This enables unauthorized access to internal services that would otherwise be protected, potentially leading to information disclosure or further compromise of the cluster environment.	2026-08-19	9.3	CVE-2026-66794

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Multicluster Engine for Kubernetes	A flaw was found in the managedcluster-import-controller. The Certificate Signing Request (CSR) auto-approval logic improperly validates incoming CSRs, specifically by not inspecting the signer name or decoding the PEM-encoded x509 CSR. This vulnerability allows a privileged service account on a spoke cluster to submit a malicious CSR. Successful exploitation can lead to privilege escalation, enabling the attacker to obtain administrative credentials on the hub cluster.	2026-08-17	9.1	CVE-2026-66795
Red Hat--Multicluster Engine for Kubernetes	A flaw was found in managed-serviceaccount. A compromised addon-manager pod, due to its ClusterRole granting excessive permissions, can read any secret across all namespaces. Additionally, it can approve arbitrary Certificate Signing Requests (CSRs), which could lead to information disclosure and privilege escalation within the cluster.	2026-08-18	8.7	CVE-2026-75924
Red Hat--Multicluster Engine for Kubernetes	A flaw was found in the clusterclaims-controller component of multicluster engine (MCE). A tenant with standard permissions to create and delete ClusterClaim resources can exploit this by manipulating the `spec.namespace` field. This allows the tenant to specify and delete any ManagedCluster, including the hub's local-cluster or other tenants' clusters, due to a missing ownership check. This vulnerability can lead to a denial of service by enabling unauthorized deletion of ManagedClusters.	2026-08-21	7.7	CVE-2026-73267
Red Hat--Multicluster Engine for Kubernetes	A flaw was found in mce-operator-bundle. The build process fetches and executes scripts from a remote repository without performing integrity checks, such as commit pinning or signature verification. This allows a malicious actor with write access to the remote repository to inject and execute arbitrary code during the build. The consequence is a compromised build process, potentially leading to the distribution of malicious software.	2026-08-19	7.7	CVE-2026-75569
Red Hat--Multicluster Global Hub	A flaw was found in the multicloud-operators-subscription component. This vulnerability allows a user on a managed cluster to escalate their privileges by creating a Subscription with specific, crafted annotations. Successful exploitation grants the attacker the ability to deploy resources into any namespace with the elevated permissions of the controller's Service Account, potentially leading to unauthorized access and control over cluster resources.	2026-08-17	9.9	CVE-2026-66792
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the submariner-operator component. The `submariner-k8s-broker-cluster` Role, which is assigned to joined clusters, possesses excessive permissions. This allows a compromised cluster to alter network configurations, specifically by overwriting other clusters' endpoint information. Consequently, an attacker can redirect inter-cluster tunnel traffic, enabling a Man-in-the-Middle (MITM) attack across the entire cluster mesh.	2026-08-18	9.9	CVE-2026-66780
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in Submariner. This vulnerability allows a malicious cluster (spoke) to redirect network traffic from other connected clusters (peer clusters) by publishing a specially crafted network endpoint. The system fails to properly validate the network subnets provided by the malicious cluster, enabling it to declare arbitrary network ranges. Consequently, all network traffic intended for these arbitrary ranges from peer clusters will be rerouted through the attacker's tunnel, potentially leading to unauthorized information disclosure or network disruption.	2026-08-20	9.9	CVE-2026-66785
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in Lighthouse. A remote attacker, by compromising a spoke cluster, can exploit a vulnerability where the destination namespace for resource injection is derived from an attacker-controlled label or annotation on the broker object. This allows the attacker to inject unauthorized EndpointSlices and ServiceImports into any namespace on peer clusters, including critical system namespaces like kube-system and openshift-*. This could lead to privilege escalation or other forms of system compromise within the cluster.	2026-08-20	9.9	CVE-2026-66788
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the multicloud-operators-subscription component. This vulnerability allows a tenant, who has the ability to create HelmRelease custom resources (CRs), to bypass existing security controls. The system's HelmRelease controller processes Helm chart templates using its own elevated ServiceAccount privileges without proper validation. This enables the tenant to deploy arbitrary resources across the entire cluster, leading to a significant security compromise.	2026-08-20	9.9	CVE-2026-67567
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in search-v2-operator. The operator's ClusterRole has permissions equivalent to a cluster administrator, allowing it to impersonate other entities, write Role-Based Access Control (RBAC) configurations, approve Certificate Signing Requests (CSRs), and manage ManifestWork. This grants excessive privileges beyond what is necessary for the operator's intended function, potentially leading to privilege escalation within the cluster.	2026-08-19	9.9	CVE-2026-70496

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the search-v2-operator. This vulnerability allows a privileged user, specifically a Custom Resource (CR) editor, to manipulate Search CR fields such as imageOverride, arguments, and environment variables without proper validation. By exploiting this, an attacker can mount arbitrary secrets into a search container's environment or replace the container image with an attacker-controlled one. This leads to privilege escalation and can result in a full cluster compromise due to the ServiceAccount's extensive impersonation permissions.	2026-08-19	9.1	CVE-2026-71470
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in acm-search-v2-rhel9. This vulnerability allows an authenticated attacker, such as a hub administrator or a Search Custom Resource (CR) editor, to inject malicious shell commands or SQL statements. This occurs because the WORK_MEM string provided in the Search CR is not properly validated before being used in a bash script and an SQL query. Successful exploitation could lead to arbitrary code execution within the privileged postgres pod, potentially compromising the system.	2026-08-17	9.1	CVE-2026-71472
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the `submariner-operator` component of Red Hat Advanced Cluster Management for Kubernetes. This vulnerability allows a cluster administrator, or any user with permissions to modify the Submariner Custom Resource (CR), to specify an unvalidated image path. This lack of validation enables an attacker to execute arbitrary code with elevated privileges across the entire cluster, including control-plane nodes, by deploying a malicious image.	2026-08-18	8.2	CVE-2026-66783
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the lighthouse component of Red Hat Advanced Cluster Management for Kubernetes. This vulnerability stems from insufficient validation of advertised IP addresses within EndpointSlice objects. A compromised spoke cluster can exploit this by creating EndpointSlices with attacker-controlled IP addresses, causing other clusters' lighthouse DNS to redirect legitimate service traffic to malicious endpoints. This enables a remote attacker to conduct transparent Man-in-the-Middle (MITM) attacks on cross-cluster service communications, potentially leading to unauthorized information disclosure and data manipulation.	2026-08-20	8.7	CVE-2026-66787
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the governance-policy-addon-controller component of Red Hat Advanced Cluster Management for Kubernetes. A user with permissions to annotate the namespaced ManagedClusterAddOn resource can override the governance-policy container image. This allows an attacker to run a controlled image with cluster-admin privileges on the managed cluster, leading to arbitrary code execution and privilege escalation.	2026-08-18	8.8	CVE-2026-66793
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in search-v2-operator. This component's `search-serviceaccount` has overly broad permissions, allowing it to impersonate users and groups across the entire cluster. If an attacker gains access to any of the pods running under this service account, they could exploit this to achieve `system:masters` access, granting them full control over the cluster.	2026-08-17	8.8	CVE-2026-70495
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in acm-operator-bundle. The build process for this component downloads and runs a script from a remote source without verifying its authenticity or integrity. This script gains access to sensitive credentials, such as GitHub access tokens and registry passwords, used in the build environment. A remote attacker could exploit this vulnerability to inject malicious code, leading to unauthorized access to build resources and potential compromise of the resulting operator bundle.	2026-08-19	8	CVE-2026-76139
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the Submariner operator. This vulnerability allows for the exposure of a long-lived broker service account (SA) bearer token within the Submariner Custom Resource (CR) specification. An attacker with access to the cluster's etcd database or through `kubect! get` commands could obtain this token. The possession of this token grants full control over the mesh network, enabling unauthorized management of network resources such as endpoints and secrets.	2026-08-18	7.8	CVE-2026-66782
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the multicloud-operators-subscription component of Red Hat Advanced Cluster Management (RHACM). A tenant with HelmRelease create permissions can exploit this vulnerability by manipulating the `secretRef.Namespace` field. This allows the `GetSecret()` function in the HelmRelease controller to fetch sensitive credentials from any namespace, which are then sent to an attacker-controlled Helm repository. This can lead to the exfiltration of credentials from arbitrary namespace Secrets, resulting in information disclosure.	2026-08-20	7.7	CVE-2026-73137
Red Hat--Red Hat Ansible	A flaw was found in the AAP Controller's HashiCorp Vault credential plugin. The kubernetes_auth() function in awx_plugins/credentials/hashivault.py reads the controller pod's Kubernetes service account token and sends it to an attacker-	2026-08-18	9.6	CVE-2026-12564

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Automation Platform 2	controlled URL when a HashiCorp Vault Secret Lookup credential with kubernetes_role authentication is tested. An authenticated attacker with credential-creation privileges can exfiltrate the service account token, gaining Kubernetes API access to the control plane namespaces with full pod CRUD and secret read permissions, including database credentials and the Django SECRET_KEY.			
Red Hat--Red Hat Ansible Automation Platform 2	A server-side request forgery (SSRF) vulnerability was found in AWX's webhook status callback mechanism. When processing GitHub pull request webhooks, AWX extracts the status callback URL (pull_request.statuses_url) from the incoming webhook payload without validating the target host against the expected Git provider. This URL is persisted in job extra variables and later used to send authenticated status updates. A user with admin role on a webhook-enabled job template can read the template's webhook signing key, forge a signed GitHub webhook payload with an arbitrary statuses_url, and cause AWX to POST status updates to an attacker-controlled or internal URL. The status update request includes the configured Git Personal Access Token (PAT) in the Authorization header, resulting in credential leakage to the attacker-specified endpoint.	2026-08-18	7.7	CVE-2026-71365
Red Hat--Red Hat build of Apache Camel 4 for Quarkus 3	A flaw was found in WildFly Elytron. Password hashing and verification normalize input with Unicode NFKC, which can collapse fullwidth characters to ASCII equivalents. A remote attacker can more easily guess affected passwords by using an ASCII-only dictionary against accounts whose passwords were intended to include those non-ASCII characters, leading to unauthorized access.	2026-08-20	7.4	CVE-2026-19611
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in the reset-credentials flow of the keycloak-services component, which is the core engine for identity and access management in Red Hat Build of Keycloak. The issue allows an unauthenticated attacker to force the password reset process for any user without needing to click the required email verification link. This can result in the attacker gaining full control over target user accounts by directly setting new credentials.	2026-08-18	9.1	CVE-2026-18963
Red Hat--Red Hat build of Keycloak 26.6	A flaw was found in the legacy client-initiated account-linking endpoint of Keycloak, a widely used open-source identity and access management solution. The mechanism used to protect the account-linking process from unauthorized requests relies on a hash that can be predicted by a malicious OIDC client. By tricking a user into authenticating, an attacker-controlled client can forge a valid linking URL to connect the victim's account to an attacker's external identity. This results in a full account takeover, allowing the attacker to log in as the victim.	2026-08-18	7.3	CVE-2026-15571
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in FreeIPA. When a trust relationship is configured between FreeIPA and Active Directory, Active Directory users can bypass authentication for FreeIPA services, including the portal, SMB server, and LDAP directory. This is possible by impersonating a client name in the Ticket Granting Service (TGS) due to FreeIPA services not verifying Privilege Attribute Certificate (PAC) certificates. This vulnerability could allow an authenticated Active Directory user to escalate their privileges within the FreeIPA domain.	2026-08-20	9.6	CVE-2026-11861
Red Hat--Red Hat Enterprise Linux 10	A privilege escalation flaw was found in FreeIPA. The uniqueness constraint enforced on Kerberos principal name attributes in the 389-ds directory server does not properly account for equivalent representations of the same principal name, allowing a user with sufficient LDAP write privileges to create a service principal that impersonates an existing privileged one. This can lead to unauthorized acquisition of Kerberos service tickets for sensitive services, potentially resulting in full domain compromise.	2026-08-20	9.1	CVE-2026-13097
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in libvirt. An unprivileged local user could exploit an integer overflow vulnerability in the NodeGetFreePages RPC handler. This flaw allows crafted values to bypass a size check, leading to an undersized memory buffer. Subsequently, real NUMA node data can overwrite this buffer. This heap buffer overflow can corrupt the root libvirt daemon's memory, potentially leading to a denial of service or local privilege escalation.	2026-08-20	7.8	CVE-2026-18917
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in FreeIPA. A remote, unauthenticated attacker can exploit this vulnerability by sending oversized form POST requests to the `/ipa/migration/migration.py` endpoint. This can force the migration handler to read attacker-controlled request bodies fully into memory, leading to increased memory usage, slower request handling, and potential service disruption or denial of service.	2026-08-20	7.5	CVE-2026-73197
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in FreeIPA. A remote, unauthenticated attacker can exploit a vulnerability in the `/ipa/i18n_messages` endpoint by sending an arbitrarily large request body. This can cause the service to consume excessive memory, leading to	2026-08-20	7.5	CVE-2026-73198

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory exhaustion, degraded responsiveness, and a denial of service (DoS) condition.			
Red Hat--Red Hat Enterprise Linux 10	A memory leak flaw was found in cockpit-ws. The login page handler leaks a heap allocation on every unauthenticated request that carries a CockpitLang cookie, allowing a remote unauthenticated attacker to exhaust memory on the host and cause a denial of service.	2026-08-19	7.5	CVE-2026-76235
Red Hat--Red Hat OpenShift AI (RHOAI)	A flaw was found in the maas-api and maas-controller ServiceAccounts within Red Hat OpenShift AI. These ServiceAccounts are granted cluster-wide permissions that exceed their operational requirements. An attacker who compromises the identity of these ServiceAccounts, either through a remote code execution vulnerability or by creating a malicious pod in the same namespace, could exploit these excessive permissions. This could lead to full cluster administrator privileges through the creation of new ClusterRoleBindings or the disclosure of sensitive information by accessing all secrets across the cluster.	2026-08-17	7.9	CVE-2026-15218
Red Hat--Red Hat OpenShift Container Platform 4	A flaw was found in Kata Containers. In configurations utilizing genpolicy for Confidential Containers guest protection, a malicious host operator can exploit insufficient validation of CreateContainer mount and storage rules. This allows them to mount arbitrary container-rootfs paths over sensitive host locations or provision arbitrary content, potentially exposing confidential information or enabling the acceptance of attacker-controlled input.	2026-08-20	8.1	CVE-2026-77176
ReichertBrothers--SimplyRETS Real Estate IDX	Unauthenticated Cross Site Scripting (XSS) in SimplyRETS Real Estate IDX <= 3.2.8 versions.	2026-08-19	7.1	CVE-2026-73354
renovatebot--renovate	Renovate versions 37.158.0 before 37.199.0 contain a command injection vulnerability in the helmv3 manager's registryAliases handling that allows attackers with commit access to execute arbitrary commands. Attackers can manipulate registryAliases keys with unquoted shell metacharacters to inject commands executed during helm repo add operations, gaining full access to Renovate's execution environment.	2026-08-19	8.8	CVE-2024-58376
renovatebot--renovate	Renovate versions >= 13.87.0 and <= 19.38.6 leak temporary repository tokens into pull request comments during certain Go Modules update failure scenarios. The issue is fixed in version 19.38.7. Anyone able to view the affected pull request comments could obtain the exposed tokens.	2026-08-19	7.5	CVE-2019-25766
renovatebot--renovate	Renovate versions >=19.180.0 and <23.25.1, when used with Azure DevOps, may expose the bot's authorization token in server or pipeline logs because the git http.extraheader=AUTHORIZATION parameter is logged without redaction. Anyone with access to saved logs could obtain the bot credentials. Fixed in 23.25.1; Azure DevOps users should revoke and regenerate credentials if logs may have been exposed.	2026-08-19	7.5	CVE-2020-37267
Repute Infosystems--BookingPress Appointment Booking Pro	Unauthenticated SQL Injection in BookingPress Appointment Booking Pro <= 6.0.2 versions.	2026-08-20	9.3	CVE-2026-68566
revmaxx--InfiniteWP Client	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in revmaxx InfiniteWP Client allows Blind SQL Injection. This issue affects InfiniteWP Client: from n/a through 1.13.9.	2026-08-20	7.6	CVE-2026-74011
Rockchip--RK3588s	Secure BootROM of RK3588s SoC is vulnerable to a time-of-check to time-of-use attack in case of booting from external media (SPI NOR or NAND, EMMC or SD). The code reads the header of the next-stage loader twice. The header contains hashes of the executable modules and is signed with a private key, the public part of which is verified against the SHA256 digest blown in the OTP. The first read is only partial and contains only the hashes of the executable modules. The second is complete, including the header signature. Although the header is verified based on the fully read data, the authenticity of the executable modules is checked against the partial data from the first read. An attacker with physical access to a device containing RK3588s SoC can easily modify the next-stage loader data on-the-fly using a low-cost SD-card or SPI NOR/NAND or EMMC emulator. Even a simple ultra low-cost circuit comprising two memory chips (containing the same data but different headers - the original and the modified one) and a multiplexer can be used to carry out an attack. This can lead to arbitrary code execution with the highest privileges available (EL3). This issue affects RK3588s: RK3588s SoC BootROM (secure) 350B20210512V100 and possibly others. As remediation apply mitigations per vendor instructions or discontinue use of the product if mitigations	2026-08-19	7.6	CVE-2024-13942

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	are unavailable https://www.rock-chips.com/a/en/products/RK35_Series/2022/0926/1660.html			
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, the cmd_learn driver of the markasjunk plugin is subject to remote code execution via crafted placeholder replacement values. This issue only affects Roundcube instances using the markasjunk plugin with its cmd_learn driver.	2026-08-17	8.8	CVE-2026-74997
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, responses from the CSS (Cascading Style Sheets) proxy were not validated, which may result in information disclosure or XSS (cross-site scripting) via MIME sniffing.	2026-08-17	7.2	CVE-2026-74998
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, mail search and LITERAL+ byte-count desynchronization could lead to information disclosure or privilege escalation via IMAP command injection.	2026-08-17	7.1	CVE-2026-75002
Roxnor--FundEngine	Unauthenticated PHP Object Injection in FundEngine <= 1.7.9 versions.	2026-08-18	9.8	CVE-2026-32470
Roxnor--FundEngine	Unauthenticated PHP Object Injection in FundEngine <= 1.7.9 versions.	2026-08-20	9.8	CVE-2026-73993
rtCamp--rtMedia for WordPress, BuddyPress and bbPress	Unauthenticated SQL Injection in rtMedia for WordPress, BuddyPress and bbPress <= 4.7.11 versions.	2026-08-20	9.3	CVE-2026-66592
runatlantis--atlantis	Atlantis is a self-hosted golang application that listens for Terraform pull request events via webhooks. From 0.19.8 until 0.45.0, Atlantis does not consistently validate user-controlled workspace values supplied through accepted repository-level atlantis.yaml configuration or authenticated /api/plan input before joining them into local workspace paths. Traversal segments can escape the intended per-pull workspace directory and cause clone preparation or other working-directory code paths to call os.RemoveAll, os.MkdirAll, or related filesystem operations on out-of-bounds directories before Terraform rejects the invalid workspace name. This can create, delete, or reuse writable paths with the privileges of the Atlantis process, causing integrity loss or denial of service. This issue is fixed in version 0.45.0.	2026-08-21	8.1	CVE-2026-64679
Saad Iqbal--License Manager for WooCommerce	Customer SQL Injection in License Manager for WooCommerce <= 3.0.18 versions.	2026-08-18	7.1	CVE-2026-73345
saleor--saleor	Saleor is an e-commerce platform. From 2.10.0rc1 until 3.21.67, 3.22.63, and 3.23.22, the account activation flow treats email verification as sufficient proof of account ownership and automatically associates anonymous commerce data with the newly activated account. An attacker can use accountRegister to create an account with a victim's email address before the victim registers. If the victim follows the activation link sent to that mailbox, Saleor activates the attacker-created account and saleor/graphql/account/mutations/account/confirm_account.py can merge anonymous orders and gift-card data for the same email address without requiring the account password or another authentication factor. The attacker can then access the merged order history and personal data, including names, addresses, and phone numbers. The patched supported lines disable automatic merging by default, while the redesigned 3.24.0 flow requires password confirmation before anonymous objects are linked. This issue is fixed in versions 3.21.67, 3.22.63, and 3.23.22.	2026-08-18	8.1	CVE-2026-44472
SEO Squirrly--SEO Plugin by Squirrly SEO	Unauthenticated Cross Site Scripting (XSS) in SEO Plugin by Squirrly SEO <= 14.2.2 versions.	2026-08-20	7.1	CVE-2026-66614
sgoudelis--ground-station	Ground Station is a browser-based suite for satellite tracking, SDR reception, hardware control, and telemetry decoding. Prior to version 0.4.13, the unauthenticated save-waterfall-snapshot Socket.IO command passes attacker-controlled snapshotName input from backend/handlers/entities/sdr.py to backend/server/snapshots.py, where os.path.join permits an absolute path or parent-directory traversal and writes attacker-controlled base64-decoded bytes outside backend/data/snapshots. An attacker can write a logging YAML file containing a logging.config.dictConfig callable factory, use the unauthenticated update-app-config operation to set log_config to that file, and invoke restart_service. During restart, backend/common/logger.py passes the YAML through resolve_log_config_path(), yaml.safe_load(), and	2026-08-19	9.8	CVE-2026-53451

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	logging.config.dictConfig(), which executes the factory with service privileges and can also cause a persistent crash loop. This issue is fixed in version 0.4.13.			
Shahjada--WPDM Premium Packages	Unauthenticated Cross Site Scripting (XSS) in WPDM - Premium Packages <= 7.0.5 versions.	2026-08-18	7.1	CVE-2026-73190
Shenzhen Cudy Technology Co., Ltd.--WR3000 2.0	Cudy WR3000 2.0 running firmware before 2.5.24 contains a hard-coded JWT HMAC signing secret vulnerability in the Mosquitto MQTT broker's authentication plugin that allows unauthenticated attackers to forge valid JWT tokens by extracting the secret from the firmware image. Attackers can use the extracted secret to craft arbitrary JWT tokens and authenticate to the MQTT broker without legitimate credentials, gaining unauthorized access to the device's mesh networking interface.	2026-08-19	9.1	CVE-2026-71960
Shenzhen Cudy Technology Co., Ltd.--WR3000 2.0	Cudy WR3000 2.0 running firmware before 2.5.24 contains an OS command injection vulnerability that allows authenticated attackers to execute arbitrary OS commands with root privileges by sending unsanitized input through the mesh MQTT command interface. The sync_command binary forwards unsanitized input directly to a shell execution sink in command.lua, enabling attackers with access to the MQTT broker to exploit the default-enabled command execution path to achieve full root-level system compromise.	2026-08-19	8.8	CVE-2026-71961
simplesamlphp--saml2	The SimpleSAMLphp SAML2 library is a PHP library for SAML2 related functionality. Prior to versions 4.19.3, 4.20.2, 5.0.6, and 6.2.1, the HTTPArtifact::receive() flow can treat an unsigned embedded SAML Response as cryptographically valid for the wrong identity provider. SOAPClient::addSSLValidator() attaches a TLS-based validator to the outer SOAP ArtifactResponse, while the embedded Response receives a validator that delegates to the outer message and is later checked against metadata selected from the embedded response issuer rather than necessarily the artifact issuer. SOAPClient::validateSSL() returns normally when the TLS public key does not match the key being validated, and SAML2\Message::validate() treats a validator call that does not throw as successful. In a multi-IdP federation, a malicious or lower-trust IdP can therefore provide an ArtifactResponse containing an unsigned Response that claims a higher-trust victim IdP as issuer and authenticate as arbitrary users with attacker-chosen assertion attributes, NameID, and session data. This issue is fixed in versions 4.19.3, 4.20.2, 5.0.6, and 6.2.1.	2026-08-19	8.7	CVE-2026-49283
simplesamlphp--saml2	The SimpleSAMLphp SAML2 library is a PHP library for SAML2 related functionality. In 4.19.2 and 4.20.2, the library permits attacker-controlled XPath transforms while processing XML signatures in specially crafted SAML messages. XPath evaluation can consume uncontrolled processing resources, allowing a remote unauthenticated attacker to deny service to any entity relying on SimpleSAMLphp or directly on the SAML2 library. The mitigation limits the number of transforms, permits only transform algorithms identified by the SAML 2.0 Core specification, and specifically rejects XPath transforms. This issue is fixed in versions 4.19.3 and 4.20.3.	2026-08-19	7.5	CVE-2026-49289
siyuan-note--siyuan	SiYuan before 3.7.4 registers Go net/http/pprof debug endpoints including heap and goroutine dumps without authentication when --mode flag is not set to exactly prod. Attackers can access /debug/pprof/heap and related endpoints to extract in-memory secrets including AccessAuthCode and AI provider API keys.	2026-08-17	9.3	CVE-2026-74799
siyuan-note--siyuan	SiYuan before v3.7.4 fails to set Content-Disposition and X-Content-Type-Options headers when serving arbitrary file assets, allowing stored cross-site scripting attacks. Authenticated attackers can upload HTML files as assets and execute scripts with full kernel API access when the workspace owner opens the asset link.	2026-08-17	9	CVE-2026-74800
siyuan-note--siyuan	SiYuan before v3.7.4 fails to validate the packageName parameter in Bazaar install and uninstall endpoints, allowing authenticated administrators to perform path traversal via directory traversal sequences. Attackers with admin access can write arbitrary files to any location via install operations or recursively delete directories via uninstall operations by supplying crafted packageName values.	2026-08-21	9.1	CVE-2026-77086
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an arbitrary file deletion vulnerability in the /api/search/removeTemplate endpoint that accepts an unvalidated path parameter passed directly to os.RemoveAll. Authenticated admin attackers can supply absolute filesystem paths to recursively delete any file or directory the kernel process has permission to remove, anywhere on the host filesystem.	2026-08-22	8.7	CVE-2026-60084
siyuan-note--siyuan	SiYuan kernel before v3.7.4 contains a path traversal vulnerability in the database_clean MCP tool. The tool performs only an empty-string check on the id parameter before passing it to RemoveUnusedAttributeView (kernel/model/attribute_view.go), which builds a filesystem path via filepath.Join	2026-08-17	8.7	CVE-2026-74798

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	without validating that id matches SiYuan's node-ID format. An authenticated MCP client can supply path traversal sequences in id to cause the kernel to copy an arbitrary file readable by the process into SiYuan's history directory (arbitrary file read) and then delete the original file (arbitrary file deletion). The corresponding HTTP API handler was hardened in GHSA-7hm9-v7vf-7g4w, but this MCP caller was not.			
siyuan-note--siyuan	SiYuan before 3.7.4 fails to properly escape workspace directory paths when constructing command-line arguments for the elevated elevator.exe helper process. Attackers can create a malicious workspace directory with command metacharacters in its path and trigger the Microsoft Defender exclusion flow to execute arbitrary commands with administrator privileges after UAC approval.	2026-08-17	8.2	CVE-2026-74801
siyuan-note--siyuan	SiYuan versions before 3.7.4 contain a cross-site WebSocket hijacking vulnerability in the admin-only /ws/network/proxy endpoint that explicitly disables origin validation by setting CheckOrigin to unconditionally return true. Attackers can craft malicious webpages that establish WebSocket connections to this endpoint and direct the SiYuan kernel process to proxy arbitrary network traffic to attacker-chosen targets, enabling authenticated network pivoting through the victim's machine.	2026-08-17	8.2	CVE-2026-74802
siyuan-note--siyuan	SiYuan before v3.7.4 contains a cross-site scripting vulnerability in the file upload validation flow that fails to escape filenames before inserting them into HTML via insertAdjacentHTML. Attackers can craft a malicious filename containing script payloads that execute with full OS command access when a user drags, drops, or pastes the file into the editor.	2026-08-18	8.6	CVE-2026-74902
siyuan-note--siyuan	SiYuan through 3.7.3 contains a cross-site scripting vulnerability in the '(!' block-reference autocomplete hint popup. In genHintItemHTML() (app/src/protyle/hint/extend.ts), a candidate block's name, alias, and memo fields are concatenated into the popup's HTML without escaping. An attacker who can set these metadata fields on a block can inject a self-firing payload (e.g.) that executes automatically when a victim types '(!' followed by a search term that surfaces the crafted block. Because SiYuan's Electron windows run with nodeIntegration enabled, contextIsolation disabled, and no CSP, the injected script gains require('child_process') access, allowing the XSS to escalate to arbitrary OS command execution.	2026-08-19	8.6	CVE-2026-75916
siyuan-note--siyuan	SiYuan before v3.7.4 contains a cross-site scripting vulnerability in the file-tree picker's hover-tooltip generation (app/src/util/pathName.ts, getLeaf()/movePathTo()) used by the 'move/link to' path-selection dialogs, where document metadata fields (bookmark, alias, memo, and an alternate name field) are concatenated into the aria-label HTML attribute without escaping. A document crafted with a double quote in any of these fields breaks out of the attribute context and injects arbitrary HTML attributes including inline event handlers (e.g., onmouseover). Because every SiYuan Electron BrowserWindow runs with nodeIntegration:true, contextIsolation:false, and no CSP, the injected handler gains require('child_process') access, escalating the XSS to arbitrary OS command execution when a victim merely hovers over the malicious document entry in the path-picker dialog. Malicious documents reach victims via sharing, sync, or import.	2026-08-19	8.6	CVE-2026-75917
siyuan-note--siyuan	SiYuan versions before 3.7.4 contain an unthrottled brute-force vulnerability in the Publish Service Basic Auth implementation (PublishServiceTransport.RoundTrip() in kernel/server/proxy/publish.go). The Publish Service runs on a separate, unauthenticated-by-default listener (default TCP port 6808) and gates named publish-viewer accounts (Conf.Publish.Auth.Accounts) with Basic Auth that has no rate limiting, per-account lockout, or backoff. Unauthenticated remote attackers can submit unlimited password guesses against named accounts to gain access to published notes/notebooks.	2026-08-17	7.5	CVE-2026-74868
siyuan-note--siyuan	SiYuan before v3.7.4 is missing authorization checks in 17 block metadata/content endpoints in kernel/api/block.go (including getRefText, checkBlockExist, and getBlockBreadcrumb). These handlers are gated only by basic authentication (model.CheckAuth) and lack publish-access filtering, allowing anonymous publish-mode readers to disclose private block content-derived text, structural metadata, and existence information for arbitrary block IDs across the workspace.	2026-08-18	7.5	CVE-2026-74904
siyuan-note--siyuan	SiYuan before v3.7.4 contains a server-side request forgery (SSRF) vulnerability in the isPrivateIP function in kernel/util/net.go, used by SSRFSafeDialer to enforce SSRF protection in SafeMode. The function only checks for loopback, link-local unicast, private, and unspecified addresses and does not recognize IPv6 transition addresses (NAT64 64:ff9b::/96, 6to4 2002::/16, Teredo 2001::/32) that embed	2026-08-18	7.1	CVE-2026-74905

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	private IPv4 destinations. When SafeMode is enabled, an authenticated attacker can bypass the SSRF guard via the network forward proxy, WebSocket proxy, or SSE proxy endpoints by supplying a URL whose hostname resolves to such a transition address, reaching internal services and cloud metadata endpoints (e.g., 169.254.169.254). Because the forward proxy returns the full response body, this is a full-read SSRF that can be used to steal instance credentials, reach internal services, and port-scan internal infrastructure.			
siyuan-note--siyuan	SiYuan before v3.7.4 contains an incorrect authorization vulnerability in eight publish-mode reader-facing endpoints that filter results using the visibility list instead of the disabled list. Anonymous visitors can discover and read content from documents explicitly marked as forbidden from publishing by accessing search, backlink, asset content, saved criteria, recent documents, graph, and tag endpoints.	2026-08-18	7.5	CVE-2026-74906
skypilot-org--skypilot	SkyPilot fails to validate that authenticated users are entitled to grant administrator roles when updating service account permissions. Attackers can create a service account, escalate it to administrator role, and authenticate with its bearer token to gain administrative control over all users and workspaces.	2026-08-17	8.8	CVE-2026-75481
SmartDataSoft--Resido	Unauthenticated Local File Inclusion in Resido <= 1.5 versions.	2026-08-19	8.1	CVE-2026-73387
smicallef--spiderfoot	SpiderFoot fails to HTML-escape correlation titles built from external scan data sources including server banners and metadata. Attackers can inject malicious HTML elements with event handlers into correlation results that execute scripts in the operator's browser when the correlations view is opened, potentially stealing API keys.	2026-08-18	9.3	CVE-2026-75626
SourceCodester--Class and Exam Timetabling System	A weakness has been identified in SourceCodester Class and Exam Timetabling System 1.0. This vulnerability affects unknown code of the file /edit_subject2.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-17	7.3	CVE-2026-75079
SourceCodester--Class and Exam Timetabling System	A security vulnerability has been detected in SourceCodester Class and Exam Timetabling System 1.0. This issue affects some unknown processing of the file /edit_subject1.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	2026-08-17	7.3	CVE-2026-75080
SourceCodester--Pet Grooming Management Software	A flaw has been found in SourceCodester Pet Grooming Management Software 1.0. This vulnerability affects unknown code of the file /admin/get_barcode_data.php. This manipulation of the argument barcode causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2026-08-17	7.3	CVE-2026-75014
SourceCodester--Simple Online Food Ordering System	A flaw has been found in SourceCodester Simple Online Food Ordering System 1.0. The impacted element is an unknown function of the file /admin/ajax.php?action=login. Executing a manipulation of the argument Username can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	2026-08-19	7.3	CVE-2026-76048
SourceCodester--Simple Online Food Ordering System	A vulnerability has been found in SourceCodester Simple Online Food Ordering System 1.0. This affects an unknown function of the file /admin/ajax.php?action=save_menu. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2026-08-19	7.3	CVE-2026-76049
SourceCodester--Simple Online Food Ordering System	A vulnerability was found in SourceCodester Simple Online Food Ordering System 1.0. This impacts an unknown function of the file /admin/ajax.php?action=delete_menu. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2026-08-19	7.3	CVE-2026-76050
SourceCodester--Simple Online Food Ordering System	A security flaw has been discovered in SourceCodester Simple Online Food Ordering System 1.0. Impacted is an unknown function of the file /fos/admin/view_order.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	2026-08-20	7.3	CVE-2026-76996
SourceCodester--Simple Online Food Ordering System	A security vulnerability has been detected in SourceCodester Simple Online Food Ordering System 1.0. The impacted element is an unknown function of the file /admin/ajax.php?action=delete_category. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	2026-08-20	7.3	CVE-2026-76998

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SpabRice--Vavo Core	Unauthenticated Local File Inclusion in Vavo Core <= 2.3.0 versions.	2026-08-18	8.1	CVE-2026-28570
SPIP--SPIP	SPIP before 4.4.20 allows unauthenticated remote attackers to execute arbitrary code, as exploited in the wild in August 2026. This is related to incorrect identification of <?php blocks, and var_export's mishandling of certain cases such as presence of a '<' character.	2026-08-20	9.8	CVE-2026-77647
SPIP--SPIP	SPIP before 4.4.21 allows unauthenticated remote attackers to execute arbitrary code, as exploited in the wild in August 2026. This is related to code injection via an X-Spip-Filtre HTTP request header that is mishandled by analyse_resultat_skel.	2026-08-21	9.8	CVE-2026-77806
Splunk--Cisco Talos Intelligence for Enterprise Security Cloud	In Cisco Talos Intelligence for Enterprise Security Cloud versions below 1.0.3, a user that holds a role with the get_talos_enrichment capability could send a crafted request to the Talos intelligence enrichment Representational State Transfer (REST) API endpoint and cause the instance to make an outbound request to an attacker-controlled server. The request could expose tokens that compromise all relevant data and system integrity in the Splunk instance. The vulnerability is possible because the Talos intelligence enrichment REST endpoint accepts the destination for authenticated Splunk management requests from request data. For more information see Deploy Cisco Talos Intelligence for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/user-guide/8.0/introduction/deploy-cisco-talos-intelligence-for-splunk-enterprise-security-cloud-only) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76389
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.0, a user who does not hold the "admin" or "power" Splunk roles could run searches with system-level privileges, access all relevant data, affect system integrity, and read or delete search jobs belonging to other users through Agent Run History. The improper privilege management is possible because the Agent Run History handler replaces the calling user session key with a system authentication token before it performs search operations. For more information see AI Toolkit Agent Launchpad (https://help.splunk.com/en/splunk-enterprise/apply-machine-learning/use-ai-toolkit/6.0.0/ai-toolkit-connections-containers-and-agents/ai-toolkit-agent-launchpad) in the Splunk documentation.	2026-08-19	8.3	CVE-2026-76391
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.0, a low-privileged user who does not hold the "admin" or "power" Splunk roles could start, stop, and configure containers, and read or modify connection and configuration data through the Representational State Transfer (REST) API. The missing authorization is possible because multiple REST API handlers in Splunk AI Toolkit do not enforce authorization checks. For more information see Troubleshoot the Splunk Machine Learning Toolkit (https://help.splunk.com/en/splunk-cloud-platform/apply-machine-learning/machine-learning-toolkit-user-guide/5.5.0/troubleshooting-mltk/troubleshoot-the-splunk-machine-learning-toolkit) in the Splunk documentation.	2026-08-19	8.3	CVE-2026-76394
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.0, a user who holds the "power" Splunk role could execute arbitrary code on the Splunk server by loading a model file containing crafted sparse matrix data. The deserialization of untrusted data is possible because a model codec in Splunk AI Toolkit deserializes sparse matrix data without guarding against embedded pickle content. For more information see Troubleshoot the Splunk Machine Learning Toolkit (https://help.splunk.com/en/splunk-cloud-platform/apply-machine-learning/machine-learning-toolkit-user-guide/5.5.0/troubleshooting-mltk/troubleshoot-the-splunk-machine-learning-toolkit) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76395
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.0, a user who holds the "power" Splunk role could access and delete all relevant data in experiment history, including data associated with other users. The vulnerability is possible because Splunk AI Toolkit does not preserve the trusted experiment scope when it processes caller-controlled query values before accessing restricted history data. For more information see Experiment Assistants (https://help.splunk.com/en/splunk-cloud-platform/apply-machine-learning/use-ai-toolkit/5.6.4/experiment-assistants) in the Splunk documentation.	2026-08-19	8.1	CVE-2026-76397
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.1, a user who holds the "power" Splunk role could modify app-provided scheduled searches to run arbitrary Search Processing Language (SPL) using the permissions of the search owner, which could allow access to all relevant data and affect system integrity. The vulnerability is possible	2026-08-19	8.1	CVE-2026-76399

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	because Splunk AI Toolkit gives the "power" Splunk role permission to modify scheduled searches that run using the permissions of the search owner.			
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.0, a user that holds a role with the schedule_search capability could cause a scheduled search to load and deserialize a model file through the apply search command. The improper access control is possible because Splunk AI Toolkit does not mark the apply search command as risky. For more information see Troubleshoot the AI Toolkit (https://help.splunk.com/en/splunk-enterprise/apply-machine-learning/use-ai-toolkit/5.7.3/troubleshooting-the-ai-toolkit/troubleshoot-the-ai-toolkit) in the Splunk documentation.	2026-08-19	7.5	CVE-2026-76396
Splunk--Splunk Connect for Kafka	In Splunk Connect for Kafka versions below 2.2.7, an unauthenticated user who can reach the Kafka Connect Representational State Transfer (REST) API could configure a non-secure Hypertext Transfer Protocol (HTTP) Event Collector endpoint in Splunk Enterprise that causes the connector to send authentication credentials to an attacker-controlled server, allowing for exposure of credentials that compromise all relevant data sent through the connector and limited alteration of event delivery. The vulnerability is possible because HTTP Event Collector endpoint validation does not require secure transport by default. For more information see Install Splunk Connect for Kafka (https://help.splunk.com/en/data-management/integrate-data-with-add-ons/splunk-connect-for-kafka/2.2/install/install-splunk-connect-for-kafka), Data ingestion parameters for Splunk Connect for Kafka (https://help.splunk.com/en/data-management/integrate-data-with-add-ons/splunk-connect-for-kafka/2.2/overview/data-ingestion-parameters-for-splunk-connect-for-kafka), and Set up and use HTTP Event Collector with configuration files (https://help.splunk.com/en/splunk-enterprise/get-data-in/get-started-with-getting-data-in/9.4/get-data-with-http-event-collector/set-up-and-use-http-event-collector-with-configuration-files) in the Splunk documentation.	2026-08-19	8.2	CVE-2026-76402
Splunk--Splunk Connect for Kafka	In Splunk Connect for Kafka versions below 2.2.7, an unauthenticated user positioned in the network path could read or alter all relevant data sent from the connector when Kerberos authentication is used with Hypertext Transfer Protocol (HTTP) Event Collector in Splunk Enterprise. The vulnerability is possible because the Kerberos authentication path does not apply the configured certificate validation options when it builds the HTTP client. For more information see Install Splunk Connect for Kafka (https://help.splunk.com/en/data-management/integrate-data-with-add-ons/splunk-connect-for-kafka/2.2/install/install-splunk-connect-for-kafka), Security configurations for Splunk Connect for Kafka (https://help.splunk.com/en/splunk-enterprise/get-data-in/splunk-connect-for-kafka/2.2/configure/security-configurations-for-splunk-connect-for-kafka), and Set up and use HTTP Event Collector with configuration files (https://help.splunk.com/en/splunk-enterprise/get-data-in/get-started-with-getting-data-in/9.4/get-data-with-http-event-collector/set-up-and-use-http-event-collector-with-configuration-files) in the Splunk documentation.	2026-08-19	7.4	CVE-2026-76403
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user who has an embedded report token could download the associated search job dispatch archive, recover session material, and use it to access all relevant data available to the report owner and affect system integrity, including by performing administrative actions when the owner holds the "admin" Splunk role. The vulnerability is possible because embedded report access does not block Representational State Transfer (REST) API dispatch archive download requests. For more information see Additional configuration for embedded reports (https://help.splunk.com/en/splunk-enterprise/create-dashboards-and-reports/reporting-manual/9.1/report-management/additional-configuration-for-embedded-reports) and About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access) in the Splunk documentation.	2026-08-19	9.4	CVE-2026-76310
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user who has an embedded report token could download the dispatch archive for an embedded report search job and use exposed session material to access all relevant data and affect system integrity on the Splunk platform instance. The vulnerability is possible because the embedded report authorization flow does not block dispatch archive download requests before Splunk Enterprise begins sending the archive to the requester. For more information see Additional configuration for embedded reports	2026-08-19	9.4	CVE-2026-76311

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(https://help.splunk.com/en/splunk-enterprise/create-dashboards-and-reports/reporting-manual/10.4/report-management/additional-configuration-for-embedded-reports) and Embed scheduled reports (https://help.splunk.com/en/splunk-enterprise/create-dashboards-and-reports/reporting-manual/10.4/report-management/embed-scheduled-reports) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.1, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user who can read the Hypertext Markup Language (HTML) source of a page that embeds a Splunk report could use exposed session material to access all relevant data and affect system integrity. The vulnerability is possible because the dispatch archive download path does not correctly enforce the embedded-report authorization boundary and includes sensitive session material in archived search-job data. For more information see Additional configuration for embedded reports (https://help.splunk.com/en/splunk-enterprise/create-dashboards-and-reports/reporting-manual/10.4/report-management/additional-configuration-for-embedded-reports) and Embed scheduled reports (https://help.splunk.com/en/splunk-enterprise/create-dashboards-and-reports/reporting-manual/10.4/report-management/embed-scheduled-reports) in the Splunk documentation.	2026-08-19	9.4	CVE-2026-76312
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user that holds a role with the schedule_search capability could run arbitrary Search Processing Language (SPL) commands with the highest level of system privilege and read every credential stored in the credential store, which can allow for disclosure and modification of all relevant data and affect system integrity and availability. The vulnerability is possible because scheduled search alert action configuration does not properly restrict user-specific alert action settings before the search scheduler runs alert actions. For more information see Create scheduled alerts (https://help.splunk.com/en/splunk-enterprise/alert-and-respond/alerting-manual/9.3/create-alerts/create-scheduled-alerts), Set up alert actions (https://help.splunk.com/en/splunk-enterprise/alert-and-respond/alerting-manual/9.3/configure-alert-actions/set-up-alert-actions), Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities), and Configuration file precedence (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.2/administer-splunk-enterprise-with-configuration-files/configuration-file-precedence) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76253
Splunk--Splunk Enterprise	In Splunk Enterprise for Windows versions below 10.4.2, 10.2.6, 10.0.9, 9.4.13, and 9.3.14, a local user with access to the Windows host could bind to the management port before Splunk Enterprise starts, intercept authentication tokens from child processes, and use those tokens to compromise all relevant data and system integrity available to the user account running Splunk Enterprise. The vulnerability is possible because the Windows management-port listener does not apply exclusive address binding protections before the service starts.	2026-08-19	8.8	CVE-2026-76259
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could perform Remote Code Execution (RCE) by uploading a malicious knowledge bundle and causing it to be used by distributed search, which can allow for access to all relevant data and affect system integrity and availability. The vulnerability is possible because the Representational State Transfer (REST) API endpoint for knowledge bundle upload does not require the high-privilege capability edit_dist_peer, and distributed search accepts caller-supplied knowledge bundle selections from users who do not hold that capability. For more information see What search heads send to search peers (https://help.splunk.com/en/splunk-enterprise/administer/distributed-search/9.2/knowledge-bundle-replication/what-search-heads-send-to-search-peers), About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/9.0/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access), Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/9.1/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities), and Using the REST API reference (https://help.splunk.com/en/splunk-enterprise/rest-api-reference/10.4/introduction/using-the-rest-api-reference) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76313

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could perform Remote Code Execution (RCE) by submitting crafted Splunk Web Manager Configuration content. The user could then access all relevant data and affect system integrity and availability. The vulnerability is possible because Splunk Web evaluates manager Extensible Markup Language expressions without sufficient input restrictions, and the associated configuration route does not require the capability expected for manager configuration changes. For more information see About configuration files (https://help.splunk.com/en/data-management/splunk-enterprise-admin-manual/10.4/administer-splunk-enterprise-with-configuration-files/about-configuration-files) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76314
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could execute arbitrary code on the Splunk platform instance through Splunk Web Manager Configuration. The user could then access all relevant data and affect system integrity and availability on the Splunk platform instance. The vulnerability is possible because Splunk Web Manager Configuration evaluates manager configuration values, and the Representational State Transfer (REST) API path for manager configuration does not require the permission that normally controls manager configuration writes. For more information see About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access) and restmap.conf (https://help.splunk.com/en/data-management/splunk-enterprise-admin-manual/10.2/configuration-file-reference/10.2.0-configuration-file-reference/restmap.conf) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76315
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.1, 10.2.5, 10.0.9, and 9.4.14, an unauthenticated user who can reach the Splunk management port could store a Search Processing Language (SPL) pipeline that runs when an administrator opens the Add Data forwarder workflow. The SPL pipeline could access all relevant data, affect system integrity, and affect availability of the Splunk platform instance. The SPL injection is possible because Deployment Server client identifiers are placed into dispatched searches without neutralizing special characters. Successful exploitation requires an administrator to open the affected Add Data forwarder workflow after the unauthenticated user registers a crafted Deployment Server client identity. For more information see Forward data (https://help.splunk.com/en/splunk-enterprise/get-started/get-data-in/10.2/how-to-get-data-into-your-splunk-deployment/forward-data) and About agent management (https://help.splunk.com/en/splunk-enterprise/administer/update-your-deployment/10.4/agent-management/about-agent-management) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76316
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could move files that the user account running Splunk Enterprise can read into a lookup that the user controls. The user could then access all relevant data and affect system integrity and availability on the search head. The vulnerability is possible because the lookup configuration endpoint does not resolve lookup source paths before checking whether they stay inside the allowed lookup staging area. For more information see About lookups (https://help.splunk.com/en/splunk-enterprise/manage-knowledge-objects/knowledge-management-manual/10.4/use-lookups-in-splunk-web/about-lookups) and Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76317
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a low-privileged user that does not hold the fsh_manage capability could perform Remote Code Execution through Federated Search bundle selection. This could allow for access to all relevant data and affect system integrity and availability. The vulnerability is possible because the Federated Search dispatch flow accepts caller-controlled bundle selection without enforcing the capability that manages federated providers and indexes. For more information see Security models for Federated Search for Splunk (https://help.splunk.com/en/splunk-enterprise/search/federated-search/10.4/run-federated-searches-across-other-splunk-deployments/service-accounts-and-security-for-federated-search-for-splunk/security-models-for-federated-search-for-splunk) and Define roles on the	2026-08-19	8.8	CVE-2026-76319

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could inject Search Processing Language (SPL) into saved-search dispatch requests. This could allow for unauthorized access to all relevant data and affect system integrity within Splunk Enterprise. The vulnerability is possible because Splunk Enterprise does not correctly validate caller-supplied time values before using them in saved-search dispatch. For more information see Search endpoint descriptions (https://help.splunk.com/en/splunk-enterprise/rest-api-reference/10.2/search-endpoints/search-endpoint-descriptions) in the Splunk documentation.	2026-08-19	8.1	CVE-2026-76331
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an authenticated user who does not hold a role with the edit_manager_xml capability could write a malicious Splunk Web Manager Extensible Markup Language (XML) configuration. When the same user opens the affected Splunk Web Manager page, Splunk Enterprise runs attacker-controlled operating-system commands as the user account running Splunk Enterprise. The vulnerability is possible because Splunk Web does not require the edit_manager_xml capability before accepting Splunk Web Manager XML configuration changes.	2026-08-19	8.8	CVE-2026-76335
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user who has access to a trusted distributed search private key could forge an administrative session token, access all relevant data, affect system integrity, and disrupt service availability. The vulnerability is possible because the distributed search authentication token endpoint does not require a signed request to identify a configured search peer, allowing the request to fall back to shared local key material. For more information see About distributed search (https://help.splunk.com/en/splunk-enterprise/administer/distributed-search/10.4/overview-of-distributed-search/about-distributed-search) and authentication.conf (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.4/configuration-file-reference/10.4.2-configuration-file-reference/authentication.conf) in Splunk documentation.	2026-08-19	8.1	CVE-2026-76338
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user that holds a role with the schedule_search capability could configure Portable Document Format (PDF) attachments in the email alert action workflow. When the email alert action runs, it could execute arbitrary Search Processing Language (SPL) commands with system-level privileges, expose all relevant data, and affect system integrity and availability on the search head. The vulnerability is possible because the search scheduler passes a system-level authentication context rather than the action owner context to the email alert action when it renders PDF attachments. For more information see alert_actions.conf (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.4/configuration-file-reference/10.4.0-configuration-file-reference/alert_actions.conf) in the Splunk documentation.	2026-08-19	8.8	CVE-2026-76350
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, and Splunk Secure Gateway versions below 3.10.9, 3.9.23, and 3.8.70, a user who does not hold the "admin" or "power" Splunk roles could use crafted report notification data to cause Splunk Secure Gateway to send a request to the Splunk Enterprise Representational State Transfer (REST) API using a system-level session token and modify the Splunk platform configuration. The user could then obtain a session token without a password and use it to access all relevant data and affect system integrity. The vulnerability is possible because Splunk Secure Gateway does not validate decoded report notification identifiers before using them to construct requests to the Splunk Enterprise REST API.	2026-08-19	8.8	CVE-2026-76351
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could create or modify a scripted lookup through generic configuration endpoints and run an installed lookup script with the permissions of the user account running Splunk Enterprise, which could allow for access to all relevant data and affect system integrity and availability. The vulnerability is possible because the generic transforms configuration endpoints do not enforce the capabilities required to create or edit external lookup definitions. For more information see Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-	2026-08-19	8.8	CVE-2026-76352

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) and limits.conf (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.4/configuration-file-reference/10.4.2-configuration-file-reference/limits.conf) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could affect system integrity and availability by sending a crafted Representational State Transfer (REST) API request that deletes or temporarily overwrites files writable by the user account running Splunk Enterprise processes on a non-captain search head cluster member. The vulnerability is possible because Search Head Clustering bundle replication does not validate the name of a replicated bundle file or neutralize NUL bytes before constructing the member bundle path. For more information see About search head clustering (https://help.splunk.com/en/splunk-enterprise/administer/distributed-search/10.4/overview-of-search-head-clustering/about-search-head-clustering), Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities), and Secure Splunk Enterprise service accounts (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/9.0/install-splunk-enterprise-securely/secure-splunk-enterprise-service-accounts) in the Splunk documentation.	2026-08-19	8.1	CVE-2026-76354
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, and 10.0.9, a user who does not hold the "admin" or "power" Splunk roles could cause the Splunk App for Splunk Observability Cloud to forward requests to Splunk Observability Cloud, including the Splunk Observability Cloud access token stored for the app. With this access, the user could view all relevant data available to that token and make limited changes to Splunk Observability Cloud content. The vulnerability does not affect Splunk Enterprise 9.4 and 9.3 versions. The vulnerability is possible because the app's Representational State Transfer (REST) API endpoint handlers do not enforce the read_o11y_content capability before forwarding requests with the stored access token. For more information see Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	7.1	CVE-2026-76251
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, 9.4.14, and 9.3.14, an unauthenticated user could cause another user to dispatch arbitrary Search Processing Language (SPL) pipelines from Dataset Explorer with the same privileges as that user, which can allow for access to all relevant data and system integrity available to that user and affect system availability. The vulnerability is possible because Dataset Explorer does not validate or escape dataset names before building SPL searches and does not apply SPL safeguards for risky commands to those searches. The vulnerability requires the attacker to phish the user by tricking them into opening the crafted link. The unauthenticated user should not be able to exploit the vulnerability at will. For more information see Explore a dataset (https://help.splunk.com/en/splunk-enterprise/manage-knowledge-objects/knowledge-management-manual/10.4/manage-and-explore-datasets/explore-a-dataset) and SPL safeguards for risky commands (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/best-practices-for-splunk-platform-security/spl-safeguards-for-risky-commands) in the Splunk documentation.	2026-08-19	7.5	CVE-2026-76254
Splunk--Splunk Enterprise	In Splunk Enterprise 10.4 versions below 10.4.2, an unauthenticated user could read Prometheus service metrics from the Edge Processor SPL2 Preview sidecar, including service details that expose relevant runtime and build metadata for the sidecar. The vulnerability does not affect Splunk Enterprise versions below 10.4. The information disclosure is possible because the Prometheus metrics endpoint in the Edge Processor SPL2 Preview sidecar lacks authentication, which lets any client that can reach the sidecar retrieve the metrics without credentials. For more information see About Splunk sidecars (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.4/splunk-sidecars/about-splunk-sidecars) in the Splunk documentation.	2026-08-19	7.5	CVE-2026-76262
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user could inject arbitrary Search Processing Language (SPL) into requests that search for events near a selected event. This could allow for unauthorized search execution. The vulnerability is possible because Splunk Web does not consistently escape caller-supplied values when it builds SPL for nearby-	2026-08-19	7.3	CVE-2026-76321

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	event searches, and embedded report access accepts those requests without the expected authorization check. For more information see Use time to find nearby events (https://help.splunk.com/en/splunk-enterprise/search/search-manual/10.2/specify-time-ranges/use-time-to-find-nearby-events) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "power" Splunk role could store a malicious ui-tour knowledge object that matches an auto-tour page name and share the object at the app level. The object can execute arbitrary JavaScript in the browser of another authenticated user who visits a standard Splunk Web page. The JavaScript could expose all relevant data and affect system integrity within the second user permissions. The Cross-Site Scripting (XSS) vulnerability is possible because Splunk Web resolves auto-tour entries from the app namespace and uses untrusted tour content when building the tour image.	2026-08-19	7.3	CVE-2026-76325
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user could trick an authenticated user into opening a crafted link to Monitoring Console. When the authenticated user opens the link, Splunk Enterprise runs attacker-controlled Search Processing Language (SPL) using the permissions of that user. The injected SPL could access data and perform actions available to that user. The vulnerability is possible because Monitoring Console does not sufficiently validate data used to build forwarder dashboard searches. The vulnerability requires the attacker to phish the user by tricking them into opening the crafted link. The unauthenticated user should not be able to exploit the vulnerability at will.	2026-08-19	7.1	CVE-2026-76330
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user could trick an authenticated user into opening a crafted link to Analytics Workspace. When the authenticated user opens the link, Splunk Enterprise runs attacker-controlled Search Processing Language (SPL) using the permissions of that user. The injected SPL could access data and perform actions available to that user. The vulnerability is possible because Analytics Workspace does not sufficiently validate data used to build searches. The vulnerability requires the attacker to phish the user by tricking them into opening the crafted link. The unauthenticated user should not be able to exploit the vulnerability at will.	2026-08-19	7.1	CVE-2026-76332
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "power" Splunk role could store a Dashboard Studio workflow action with a crafted Uniform Resource Locator (URL). When another authenticated user selects the stored action from Event Actions and selects Continue, attacker-controlled JavaScript runs in the browser of that user. This could expose data or actions available through Splunk Web to that user. The vulnerability is possible because Dashboard Studio does not sufficiently validate workflow-action URLs before processing them. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who holds the "power" Splunk role should not be able to exploit the vulnerability at will. For more information see Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	7.1	CVE-2026-76333
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2 and 10.2.6, a user who does not hold the "admin" or "power" Splunk roles could delete all Search Processing Language 2 (SPL2) modules across all apps and users on the instance through the SPL2 module management Representational State Transfer (REST) API. This could delete exported datasets and functions, affect system integrity, and cause partial service disruption. The vulnerability does not affect Splunk Enterprise versions below 10.2. The vulnerability is possible because the SPL2 module management REST API does not sufficiently authorize and validate module deletion requests. For more information see Manage SPL2 modules (https://help.splunk.com/en/splunk-enterprise/search/spl2-search-manual/multiple-searches-in-an-spl2-module/manage-spl2-modules) and Module permissions (https://help.splunk.com/en/splunk-enterprise/search/spl2-search-manual/modules-statements-and-views/module-permissions) in the Splunk documentation.	2026-08-19	7.1	CVE-2026-76336
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could write dispatch metadata	2026-08-19	7.7	CVE-2026-76344

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to an arbitrary location on the host by supplying a crafted search identifier to a Representational State Transfer (REST) API endpoint and affect system integrity on the host. The vulnerability is possible because Splunk Enterprise does not validate the search identifier before using it to create a dispatch directory. For more information see About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise 10.4 versions below 10.4.2, an unauthenticated user could retrieve the information contained in Edge Processor pipeline configurations through a Representational State Transfer (REST) API endpoint when Edge Processor is turned on. The vulnerability does not affect versions prior to 10.4. The vulnerability exists because the Edge Processor service endpoint lacks authentication controls. For more information see System architecture of the Edge Processor solution (https://help.splunk.com/en/splunk-enterprise/process-data-at-the-edge/use-edge-processors-for-splunk-enterprise/10.4/how-the-edge-processor-solution-works/system-architecture-of-the-edge-processor-solution) in the Splunk documentation.	2026-08-19	7.5	CVE-2026-76355
Splunk--Splunk Enterprise Security	In Splunk Enterprise Security versions below 8.6.1, a user who holds a Splunk Enterprise Security role that contains the mc_investigation_read capability could inject Search Processing Language (SPL) through Analyst Queue search filters, allowing for access to all relevant data and system integrity available to the scheduled searches that run for that user. The vulnerability is possible because the Analyst Queue search filter handling does not validate filter field names before the fields are included in SPL searches. For more information see Users and roles for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/install/8.4/installation/users-and-roles-for-splunk-enterprise-security), Manage analyst workflows using the analyst queue in Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.4/mission-control/manage-analyst-workflows-using-the-analyst-queue-in-splunk-enterprise-security), and Overview of Mission Control in Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/user-guide/8.5/mission-control/overview-of-mission-control-in-splunk-enterprise-security) in the Splunk documentation.	2026-08-19	8.1	CVE-2026-76387
Splunk--Splunk Enterprise Security	In Splunk Enterprise Security versions below 8.6.1, a user who holds the ess_analyst Splunk Enterprise Security role could change User and Entity Behavior Analytics (UEBA) search macros that scheduled searches run with administrator permissions, allowing for access to all relevant data and system integrity through those searches. The vulnerability is possible because the UEBA app metadata grants analyst roles write access to search macros that should be writable only by administrator roles. For more information see Users and roles for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/install/8.4/installation/users-and-roles-for-splunk-enterprise-security) and Roles and knowledge objects in UEBA for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.5/user-and-entity-behavior-analytics/roles-and-knowledge-objects-in-ueba-for-splunk-enterprise-security) in the Splunk documentation.	2026-08-19	8.1	CVE-2026-76388
Splunk--Splunk MCP Server app	In Splunk MCP Server app versions below 1.2.1, a user who holds the "admin" Splunk role could execute arbitrary commands on the underlying operating system. The vulnerability is possible because of missing input validation in the app's credential management component, which deserializes stored data without checking whether the content is of the expected type.	2026-08-19	9.1	CVE-2026-76404
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, an unauthenticated user could spoof the source IP address in a crafted request to an Automation Broker notification endpoint and execute arbitrary code on the Splunk SOAR host. The vulnerability is possible because the Splunk SOAR Automation Broker trusts a client-supplied source IP address header as proof that the request originates from the local system. Successful exploitation can expose all relevant data, affect system integrity, and disrupt service availability. For more information see About Splunk SOAR Automation Broker (https://help.splunk.com/en/splunk-soar/splunk-automation-broker/about-splunk-soar-automation-broker/about-splunk-soar-automation-broker) in the Splunk documentation.	2026-08-19	8.1	CVE-2026-76356
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, an authenticated user with no role assigned could submit a crafted file path to the Representational State Transfer (REST) API	2026-08-19	7.6	CVE-2026-76357

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and execute arbitrary code. The vulnerability is possible because the REST API does not require an assigned role for the request and does not restrict the user-supplied file path to the intended temporary directory. For more information see Manage roles and permissions in Splunk SOAR (On-premises) (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/manage-your-splunk-soar-on-premises-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-on-premises) and Splunk SOAR (On-premises) security information (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/introduction-to-splunk-soar-on-premises/splunk-soar-on-premises-security-information) in the Splunk documentation.			
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, an unauthenticated user who can observe or alter network traffic between Splunk SOAR and a configured CyberArk Representational State Transfer (REST) server could access or modify all relevant data exchanged through that credential manager. The vulnerability is possible because the CyberArk REST client does not verify server certificates by default. The attack requires the attacker to have network-path interception capability between Splunk SOAR and the configured CyberArk REST server. For more information see Manage your organization's credentials with a password vault (https://help.splunk.com/en/splunk-soar/soar-cloud/administer-soar-cloud/configure-administration-settings-in-splunk-soar-cloud/manage-your-organizations-credentials-with-a-password-vault) in the Splunk documentation.	2026-08-19	7.4	CVE-2026-76362
SPLWare--esProc	A vulnerability was found in SPLWare esProc up to 20260507. This affects the function ObjectInputStream.readUnshared of the file src/main/java/com/scudata/parallel/SocketData.java. Performing a manipulation results in deserialization. Remote exploitation of the attack is possible.	2026-08-19	7.3	CVE-2026-75987
Spring--Spring AI	The MCP Streamable HTTP server transport (WebFlux and WebMvc variants) does not place any limit on the number of sessions it retains, and by default does not require clients to be authenticated. As a result, a remote attacker can cause the server to accumulate an unbounded number of sessions over time, gradually exhausting available memory and ultimately causing a Denial of Service that affects all legitimate clients. Affected versions: Spring AI: 2.0.0	2026-08-21	7.5	CVE-2026-59279
sshnet--SSH.NET	SSH.NET is a Secure Shell (SSH) library for .NET. In 2025.1.0 and earlier, ScpClient.Download(string directoryName, DirectoryInfo directoryInfo) trusts file and directory names returned by a remote SCP server and combines them with the requested local directory without containment validation, allowing a malicious, compromised, or man-in-the-middle server to use ../ sequences or absolute paths to create or overwrite files anywhere writable by the client process. This issue is fixed in version 2026.0.0.	2026-08-18	7.1	CVE-2026-48798
SSL Zen--SSL Zen	Unauthenticated Cross Site Scripting (XSS) in SSL Zen <= 4.7.43 versions.	2026-08-18	7.1	CVE-2026-28569
Stefano Lissa--Newsletter	Unauthenticated Cross Site Scripting (XSS) in Newsletter <= 9.3.3 versions.	2026-08-19	7.1	CVE-2026-66596
Stirling-Tools--Stirling-PDF	Stirling-PDF is a locally hosted web application that facilitates various operations on PDF files. Prior to 2.0.0, the Get Info workflow in app/core/src/main/resources/templates/security/get-info-on-pdf.html inserts untrusted PDF Title and Author metadata into the summary-text element with innerHTML, allowing a malicious PDF to execute stored cross-site scripting when a user clicks Get Info and to access browser-session data or modify page content. This issue is fixed in version 2.0.0.	2026-08-17	8.1	CVE-2026-33437
Stirling-Tools--Stirling-PDF	Stirling-PDF is a locally hosted web application that facilitates various operations on PDF files. Prior to 2.9.0, the /api/v1/pipeline/handleData endpoint in app/core/src/main/java/stirling/software/SPDF/controller/api/pipeline/PipelineProcessor.java injects the STIRLING-PDF-BACKEND-API-USER API key into pipeline subrequests, allowing an authenticated ROLE_USER to retrieve the key through /api/v1/user/get-api-key, impersonate the internal service account, bypass normal rate limits, and access internal endpoints including /api/v1/info/requests/all and /api/v1/info/load/all. This issue is fixed in version 2.9.0.	2026-08-17	8.5	CVE-2026-57485
Stitchexpress--Stitch Express	Unauthenticated Broken Access Control in Stitch Express <= 1.9.0 versions.	2026-08-19	7.5	CVE-2026-73394
stoatchat--stoatchat	stoatchat before 0.15.0 contains a missing authorization vulnerability in the Subscribe message handler that allows authenticated attackers to enumerate members and monitor profile updates of private servers without membership. Attackers can subscribe to any server's member-update topic by sending a Subscribe message with an arbitrary server ID, receiving live UserUpdate events	2026-08-17	7.7	CVE-2026-74869

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	including display names, avatars, and status changes for members they should not have access to.			
strongSwan--strongSwan	In strongSwan before 6.0.7, identity parsing/cloning is mishandled. Parsed EAP-Identities that result in an empty but non-NULL encoding are not correctly cloned and trigger a double-free once the duplicates are destroyed.	2026-08-22	7.5	CVE-2026-47895
strukturag--libheif	libheif is a HEIF and AVIF file format decoder and encoder. From 1.19.0 until 1.23.0, a crafted HEIF sequence accepted by heif_context_read_from_memory() with the msf1 sequence brand can cause unbounded heap allocation. In libheif/sequences/seq_boxes.cc, Box_stsz::parse() applies max_sequence_frames only to variable-size samples, so fixed-size mode accepts an attacker-controlled sample_count without a bound. In libheif/sequences/track.cc, Track::load() also adds current_sample_idx and samples_per_chunk in 32-bit arithmetic, allowing the consistency check to be bypassed by wraparound. The resulting values reach the Chunk::Chunk() allocation path, which can consume gigabytes of memory and crash or stall the process through memory exhaustion. This issue is fixed in version 1.23.0.	2026-08-18	7.5	CVE-2026-50142
super-productivity--super-productivity	Super Productivity is an advanced todo list app with integrated timeboxing and time tracking capabilities. Prior to 18.13.0, the EXEC IPC handler in electron/ipc-handlers/exec.ts accepts a command string from the renderer through the IPC.EXEC channel and executes it with child_process.exec(). The electron/preload.ts bridge exposes window.ea.exec() to renderer code, including community plugins executed with new Function(), without requiring nodeExecution permission. A confirmation dialog protects only the first execution, its persistence checkbox is selected by default, and approved commands are stored in the ALLOWED_COMMANDS value in simpleSettings for silent later execution with the desktop account's privileges. This issue is fixed in version 18.13.0.	2026-08-18	7.8	CVE-2026-71551
supsysic--Contact Form by Supsysic	Unauthenticated Cross Site Scripting (XSS) in Contact Form by Supsysic < 1.10.0 versions.	2026-08-18	7.1	CVE-2026-73378
supsysic--Easy Google Maps	Unauthenticated PHP Object Injection in Easy Google Maps <= 1.13.0 versions.	2026-08-18	9.8	CVE-2026-73366
supsysic--Easy Google Maps	Unauthenticated Remote File Inclusion in Easy Google Maps < 1.14.2 versions.	2026-08-18	7.2	CVE-2026-73367
supsysic--Popup by Supsysic	Unauthenticated PHP Object Injection in Popup by Supsysic <= 1.13.0 versions.	2026-08-18	9.8	CVE-2026-73380
supsysic--Popup by Supsysic	Unauthenticated Broken Authentication in Popup by Supsysic <= 1.13.0 versions.	2026-08-18	9.1	CVE-2026-73381
supsysic--Ultimate Maps by Supsysic	Unauthenticated PHP Object Injection in Ultimate Maps by Supsysic < 1.5.0 versions.	2026-08-18	9.8	CVE-2026-73376
supsysic--Ultimate Maps by Supsysic	Unauthenticated Cross Site Scripting (XSS) in Ultimate Maps by Supsysic < 1.5.0 versions.	2026-08-18	7.1	CVE-2026-73375
supsysic--Ultimate Maps by Supsysic	Unauthenticated Broken Access Control in Ultimate Maps by Supsysic < 1.5.0 versions.	2026-08-18	7.5	CVE-2026-73377
SWE-agent--SWE-agent	SWE-agent's trajectory inspector (sweagent inspector), confirmed in v1.1.0, is an HTTP server that joins request paths to the trajectory directory in its /trajectory/ handler without rejecting parent-directory ('..') references, bypassing the built-in path sanitization. The server binds all interfaces (0.0.0.0), applies wildcard CORS, and requires no authentication. An unauthenticated network client (or a malicious web page via CORS) can use path traversal sequences to read files outside the intended directory. Because the read sink parses targets as trajectory JSON, disclosure is constrained to JSON files shaped like a trajectory, which can contain repository contents, command output, and secrets/API keys.	2026-08-17	7.5	CVE-2026-75482
Syed Balkhi--Charitable	Unauthenticated Broken Access Control in Charitable <= 1.8.11.3 versions.	2026-08-18	7.5	CVE-2026-73994
t8y2--dbx	dbx is a cross-platform database client for databases. Prior to 0.5.51, dbx-web auth_middleware in crates/dbx-web/src/auth.rs passes every protected request to the handler chain when password_hash is None. A fresh deployment reaches that state when DBX_PASSWORD is unset and no stored password exists, while crates/dbx-web/src/main.rs binds the service to 0.0.0.0 on port 4224 by default. An unauthenticated network attacker can call the /api/connection/connect and /api/query/execute routes to use configured database credentials and execute arbitrary SQL, allowing disclosure, modification, or destruction of data in connected databases. The desktop Tauri application is not affected because it binds only to loopback. This issue is fixed in version 0.5.51.	2026-08-20	9.8	CVE-2026-55642

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Tagembed--Tagembed	Unauthenticated Cross Site Scripting (XSS) in Tagembed <= 7.4 versions.	2026-08-20	7.1	CVE-2026-66590
TaxoPress--TaxoPress	Deserialization of Untrusted Data vulnerability in TaxoPress allows Object Injection. This issue affects TaxoPress: from n/a through 3.51.0.	2026-08-18	8.8	CVE-2026-74012
tclahr--uac	UAC (Unix-like Artifacts Collector) versions prior to 3.3.0 contain a command injection vulnerability in the _run_command function that allows attackers to execute arbitrary commands by injecting shell metacharacters into untrusted data such as usernames, process names, or filenames. Attackers can exploit this vulnerability through crafted evidence inputs, mounted images with hostile filenames, or tampered artifact definitions to achieve remote code execution on the analyst's host when processing evidence.	2026-08-21	7.8	CVE-2026-41449
tclahr--uac	UAC (Unix-like Artifacts Collector) versions prior to 3.3.0 contain a command injection vulnerability in the _command_collector function where foreach command output lines are substituted directly into command strings via sed without proper escaping before being evaluated with eval. Attackers can exploit this by crafting malicious filenames or artifact definitions containing shell metacharacters such as command substitution syntax or semicolons to execute arbitrary commands on the analyst's host system.	2026-08-21	7.8	CVE-2026-41450
tclahr--uac	UAC (Unix-like Artifacts Collector) versions prior to 3.3.0 contain a command injection vulnerability in the user substitution logic within parse_artifact.sh where usernames and home directories from /etc/passwd are substituted directly into command strings without escaping before execution via eval. Attackers can inject shell metacharacters such as command substitution syntax or semicolons through crafted usernames or home directory paths in /etc/passwd entries to execute arbitrary commands on the analyst's host system.	2026-08-21	7.8	CVE-2026-41451
Tecnativa--docker-socket-proxy	docker-socket-proxy fails to properly gate read endpoints in the /containers Docker API namespace when the CONTAINERS environment variable is set. Attackers can use GET requests to /containers/{id}/archive, /containers/{id}/export, /containers/{id}/logs, and /containers/{id}/top to read arbitrary files and download entire container filesystems as tar archives.	2026-08-22	7.4	CVE-2026-78122
TeconceTheme--Mayosis Core	Unauthenticated Cross Site Scripting (XSS) in Mayosis Core <= 5.4.7 versions.	2026-08-18	7.1	CVE-2026-32333
TeconceTheme--Nikstore Core	Unauthenticated SQL Injection in Nikstore Core <= 1.5 versions.	2026-08-19	9.3	CVE-2026-73388
Tenda--CH22	A vulnerability has been found in Tenda CH22 1.0.0.1. The affected element is the function formcreateFileName of the file /goform/formcreateFileName. The manipulation of the argument fileNameMit leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2026-08-20	7.4	CVE-2026-77031
Tenda--CH22	A security flaw has been discovered in Tenda CH22 1.0.0.1. The impacted element is the function formeditFileName of the file /goform/editFileName. The manipulation of the argument editNameMit results in command injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-08-23	7.4	CVE-2026-78063
Tenda--CH22	A vulnerability has been found in Tenda CH22 1.0.0.1. This affects the function formexeCommand of the file /goform/exeCommand. The manipulation of the argument cmdinput leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2026-08-23	7.4	CVE-2026-78141
tensorzero--tensorzero	TensorZero is an open-source LLM Ops platform that unifies an LLM gateway, observability, evaluation, optimization, and experimentation. Prior to 2026.6.0, the TensorZero Gateway /internal/object_storage endpoint accepts a caller-supplied JSON storage_path parameter that dynamically overrides the [object_storage] configuration. Selecting the filesystem storage type allows arbitrary files on the gateway filesystem to be read, including credential files. Selecting the s3_compatible storage type causes outbound object-storage requests to attacker-chosen internal or cloud-metadata endpoints. Exploitation requires access to the gateway, which can be authenticated or unauthenticated depending on deployment configuration. This issue is fixed in version 2026.6.0.	2026-08-21	7.7	CVE-2026-54457
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to 2.3.2, the DELETE /ssh/tunnel/disconnect/:tunnelName teardown path in src/backend/ssh/tunnel.ts interpolates endpointPort, sourcePort, endpointUsername, and endpointIP into single-quoted pkill -f patterns. An authenticated user who can edit a tunnel host field can include a single quote to terminate the pattern and append a shell	2026-08-19	9.8	CVE-2026-53545

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	command, which executes when the tunnel is disconnected. Successful exploitation runs arbitrary commands on the source SSH host with the privileges of the connected SSH account. This issue is fixed in version 2.3.2.			
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to 2.3.2, the terminal WebSocket accepts a user-controlled hostConfig.id and src/backend/ssh/host-resolver.ts resolves that host without requiring ownership or explicit access. When no credential is shared with the requester, resolveHostById performs an owner credential fallback, and src/backend/ssh/terminal.ts combines that credential with attacker-controlled ip, port, and username values. An authenticated low-privileged user can therefore make Termix authenticate to an attacker-controlled SSH server and disclose another user's stored SSH password or private-key material while the victim user's data key is unlocked. This issue is fixed in version 2.3.2.	2026-08-19	9.6	CVE-2026-53546
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to 2.6.1, the GET /host/db/host/:id/password endpoint in src/backend/database/routes/host.ts accepts an authenticated user's numeric host ID and the field=password or field=sudoPassword query without enforcing host ownership during credential resolution. A failed requester-scoped lookup can resolve the host with the owner's context and return the owner's plaintext credential, allowing any authenticated user with a valid JWT to enumerate sequential hosts.id values and retrieve SSH or sudo passwords belonging to other users. The disclosed credentials can then be used to access and control managed systems outside the Termix instance. This issue is fixed in version 2.6.1.	2026-08-19	9.6	CVE-2026-53548
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to 2.3.2, the archive creation endpoint in src/backend/ssh/file-manager.ts passes selected file basenames to tar without an end-of-options marker and without making the operands unambiguously relative. A user with access to an SSH file-manager session can select basenames beginning with GNU tar options such as --checkpoint=1 and --checkpoint-action=exec, causing tar, tar.gz, tar.bz2, or tar.xz creation to interpret those names as options. The resulting checkpoint action executes commands on the managed SSH host with the privileges of the connected SSH account, allowing file disclosure, modification, and service disruption. This issue is fixed in version 2.3.2.	2026-08-19	8.8	CVE-2026-53542
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to 2.3.2, the POST /database/export endpoint creates a user export that includes the global settings table even though the rest of the export is user-scoped. The settings table contains reset_code_ and temp_reset_token_ password-reset artifacts, allowing a low-privileged authenticated user to recover another local account's reset code and complete the normal password-reset flow. Successful exploitation results in local-user account takeover and administrative compromise when the victim is an administrator. This issue is fixed in version 2.3.2.	2026-08-19	8.8	CVE-2026-53547
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to 2.3.2, the POST /host/db/proxy/test endpoint accepts the singleProxy, proxyChain, and testTarget request fields without validating their destination addresses. The testProxyConnectivity path uses raw TCP and SOCKS connections to attacker-selected hosts and ports, allowing an authenticated user to probe localhost, private networks, link-local metadata services, and other infrastructure reachable from the Termix server. Structured connection errors disclose host reachability and timing information, and successful metadata access can expose cloud credentials. This issue is fixed in version 2.3.2.	2026-08-19	7.7	CVE-2026-53549
The Browser Company of New York--ArcSearch	ArcSearch for iOS versions prior to 1.48.0 could keep the address bar hidden after a page-initiated scroll, allowing attacker-controlled content to imitate browser interface elements and increasing spoofing risk.	2026-08-18	7.4	CVE-2026-18534
the-momentum--open-wearables	A vulnerability was identified in the-momentum open-wearables up to 0.6.2. This impacts the function redeem_invitation_code of the file backend/app/api/routes/v1/user_invitation_code.py of the component Public Invitation-Code Redemption Endpoint. The manipulation of the argument code leads to missing authentication. Remote exploitation of the attack is possible. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-23	7.3	CVE-2026-78154
The4--Kalles Addons	Unauthenticated PHP Object Injection in Kalles Addons <= 1.0.6 versions.	2026-08-19	9.8	CVE-2026-73389

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
themagnifico52--Smart Cleaning	Subscriber Arbitrary File Upload in Smart Cleaning <= 4.8.6 versions.	2026-08-20	9.9	CVE-2026-74016
themagnifico52--Warehouse Cargo	Subscriber Arbitrary File Upload in Warehouse Cargo <= 2.6.9 versions.	2026-08-20	9.9	CVE-2026-74018
thembay--Aora	Unauthenticated Cross Site Scripting (XSS) in Aora <= 1.3.19 versions.	2026-08-20	7.1	CVE-2026-66612
Theme-One Inc.--The Grid	Subscriber Privilege Escalation in The Grid <= 2.7.9.1 versions.	2026-08-18	8.8	CVE-2026-28191
ThemeComplete--Extra Product Options & Add-Ons for WooCommerce	Unauthenticated Arbitrary File Download in Extra Product Options & Add-Ons for WooCommerce < 7.6 versions.	2026-08-18	7.5	CVE-2026-73181
ThemeGoods--Capella	Unauthenticated SQL Injection in Capella <= 2.5.5 versions.	2026-08-20	9.3	CVE-2025-15688
ThemeGoods--Capella	Unauthenticated Privilege Escalation in Capella <= 2.5.5 versions.	2026-08-20	9.8	CVE-2025-15689
ThemeGrill--SmartSMTP	Unauthenticated Cross Site Scripting (XSS) in SmartSMTP <= 1.2.0 versions.	2026-08-20	7.1	CVE-2026-66606
ThemeHunk--Advance Product Search	Unauthenticated Cross Site Scripting (XSS) in Advance Product Search <= 1.4.8 versions.	2026-08-20	7.1	CVE-2026-66607
ThemetechMount--TrueBooker	Unauthenticated Privilege Escalation in TrueBooker <= 1.2.6 versions.	2026-08-19	9.8	CVE-2026-73347
themetechmount--TrueBooker Appointment Booking and Scheduler System	The TrueBooker - Appointment Booking and Scheduler System plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key leading to Account Takeover in all versions up to, and including, 1.2.6. This is due to the admin_user_create_cus AJAX handler lacking any authentication or capability check before passing the attacker-supplied truebooker_wp_user_id parameter directly to wp_update_user. This makes it possible for unauthenticated attackers to overwrite the email address of any WordPress user - including an administrator - and then complete the standard WordPress lost-password flow to fully take over the targeted account.	2026-08-19	9.8	CVE-2026-18315
Themeum--Kirki	Unauthenticated Cross Site Scripting (XSS) in Kirki <= 6.2.3 versions.	2026-08-18	7.1	CVE-2026-66629
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7 stores password reset tokens in a publicly accessible tracking file when user tracking is enabled. Unauthenticated attackers can read the tracking file at content/core/data/trackingDDMMYYYY to extract reset tokens and replay them against the password reset API to take over user accounts.	2026-08-19	8.8	CVE-2026-75918
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7 contains a SQL injection vulnerability in the glossary create and update endpoints caused by truncating an escaped string before embedding it in a SQL literal. Authenticated users with glossary add or edit permissions can craft a payload with a dangling backslash to escape the closing quote and inject arbitrary SQL commands to read sensitive database information.	2026-08-19	8.1	CVE-2026-76205
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7 contains a two-factor authentication bypass vulnerability where remember-me tokens are issued before 2FA verification completes. Attackers with valid credentials can obtain a remember-me cookie, skip the 2FA challenge, and replay the cookie to gain full authenticated access without second-factor verification.	2026-08-19	8.1	CVE-2026-76207
thorsten--phpMyFAQ	phpMyFAQ versions 3.1.0 through 4.1.6 contain an authentication bypass vulnerability in AuthLdap::create(). When LDAP authentication is enabled, after a successful LDAP bind the code calls User::setStatus('active') unconditionally, which overwrites the account_status column of a pre-existing local account from 'blocked' to 'active'. As a result, a user whose local phpMyFAQ account has been administratively blocked can restore their account and log in by authenticating via LDAP. The state transition is not logged, so administrators cannot detect that the block was overridden. Fixed in 4.1.7.	2026-08-19	8.2	CVE-2026-76208
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7 contains a brute-force vulnerability in the two-factor authentication step where the failure counter is session-scoped and reset on each successful password re-authentication. Attackers with a valid password can bypass the five-attempt limit by obtaining a fresh session cookie and repeatedly re-authenticating to reset the counter, enabling unbounded TOTP code guessing.	2026-08-19	7.4	CVE-2026-76213
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7 fails to persist the WebAuthn login challenge generated by prepareForLogin, because neither WebAuthn controller saves the mutated key objects back to the database. At login the anti-replay comparison is skipped by its own null guard, allowing an attacker who captures a successful WebAuthn	2026-08-19	7.4	CVE-2026-76214

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	assertion to replay it indefinitely and authenticate as the user without any interaction or hardware key.			
tier4--nebula	TIER IV Nebula through 1.2.0 contains an out-of-bounds read vulnerability in the Vlp32Decoder::unpack() function that allows unauthenticated remote attackers to cause the decoder to read past the end of a received UDP buffer into adjacent heap memory by sending a short UDP datagram. Attackers can send a malformed datagram to the Velodyne UDP sensor port, which lacks sender-address restrictions present in other drivers, causing fabricated points derived from heap memory contents to be silently published into downstream PointCloud2 messages consumed by Autoware nodes.	2026-08-17	7.5	CVE-2026-74238
tirr-c--jxl-oxide	jxl-oxide is a pure Rust implementation of a JPEG XL decoder. Prior to jxl-grid 0.6.2, decoding a crafted JPEG XL image on a 32-bit platform can overflow length calculations in AlignedGrid::with_alloc_tracker and related grid and subgrid arithmetic. A 65536 x 65536 frame can pass the frame-area limit while overflowing the usize element count, causing modular, VarDCT, or filter rendering paths to allocate a backing buffer smaller than the logical grid. A tiny bitstream-controlled cropped frame combined with a huge canvas or requested region can also reach the vulnerable composition path in crates/jxl-render/src/blend.rs through ordinary render_frame(). Later mutable subgrid and raw-pointer operations can then perform attacker-controlled out-of-bounds writes, causing memory corruption, denial of service, or arbitrary code execution. This issue is fixed in jxl-grid version 0.6.2.	2026-08-19	7.3	CVE-2026-52834
torproject--Tor	Tor before 0.4.9.11 is prone to a race condition where in just the right circumstances a rendezvous point could man-in-the-middle (impersonate) the onion service that the client was trying to reach.	2026-08-20	8.9	CVE-2026-77638
torproject--Tor	Tor before 0.4.9.10 did not reject a CONFLUX_LINK cell that arrives on a circuit which already has attached streams. A malicious client could send a RELAY_COMMAND_BEGIN before the CONFLUX_LINK on the same circuit, attaching an exit stream that would later end up orphan leaving a dangling circuit back-pointer and a use-after-free (UAF) when the circuit is freed. This is TROVE-2026-025.	2026-08-20	7	CVE-2026-77584
torproject--Tor	tor before 0.4.9.9 was prone to an out-of-bounds write when parsing a consensus or detached signature with unexpected signature digest type. Impact is minor for most Tor roles, but potentially major for directory authorities. This is TROVE-2026-019.	2026-08-20	7.5	CVE-2026-77642
TRENDnet--Router	A flaw has been found in TRENDnet Router 1.1.02b01. The affected element is an unknown function of the file /cgi-bin/ping.cgi. This manipulation of the argument wan_type causes command injection. The attack may be initiated remotely. The exploit has been published and may be used.	2026-08-19	7.4	CVE-2026-75985
TRENDnet--TEW-755AP	A vulnerability was found in TRENDnet TEW-755AP up to 20260702. Affected is the function FUN_401000 of the file /sbin/mycli. The manipulation of the argument ssid results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	2026-08-19	9.9	CVE-2026-76589
TRENDnet--TEW-755AP	A vulnerability was identified in TRENDnet TEW-755AP up to 20260702. Affected by this issue is some unknown functionality of the file /cgi-bin/wan.cgi of the component ssi. Such manipulation of the argument cameo.wan.wan_pppoe_password_00 leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used.	2026-08-19	9.9	CVE-2026-76590
TRENDnet--TEW-755AP	A security flaw has been discovered in TRENDnet TEW-755AP up to 20260702. This affects the function log_email_server of the file /cgi-bin/email.cgi of the component ssi. Performing a manipulation results in command injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	2026-08-19	7.4	CVE-2026-76591
TRENDnet--TEW-821DAP	A vulnerability was determined in TRENDnet TEW-821DAP 2.2.01b05. Affected by this vulnerability is the function uci_safe_get of the file /cgi-bin/apply_time.cgi of the component NTP Timezone Configuration Handler. Executing a manipulation of the argument system.ntp.server/system.ntp.enable_server/cameo.time.time_zone/cameo.cameo.syslog_server can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-22	10	CVE-2026-77946
TRENDnet--TEW-821DAP	A vulnerability was determined in TRENDnet TEW-821DAP 2.2.01b05. Affected is the function popen/system of the file /cgi-bin/ping.cgi of the component ssi. Executing a manipulation of the argument ipaddr can lead to command injection. It	2026-08-19	7.4	CVE-2026-76582

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.			
TRENDnet--TEW-821DAP	A vulnerability was found in TRENDnet TEW-821DAP 2.2.01b05. Affected is an unknown function of the file /cgi-bin/upload.cgi of the component ssi. Performing a manipulation of the argument filename results in command injection. The attack may be initiated remotely. The exploit has been made public and could be used.	2026-08-22	7.4	CVE-2026-77945
TRENDnet--TEW-823DRU	A weakness has been identified in TRENDnet TEW-823DRU 1.1.02b01. Impacted is the function strcpy of the file /cgi-bin/wan.cgi of the component NVRAM. This manipulation of the argument wan_l2tp_password causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-18	9.9	CVE-2026-75976
TRENDnet--TEW-823DRU	A vulnerability was detected in TRENDnet TEW-823DRU 1.1.02b01. Impacted is an unknown function of the file /cgi-bin/admin.cgi. The manipulation of the argument Hostname results in command injection. The attack can be launched remotely. The exploit is now public and may be used.	2026-08-19	7.4	CVE-2026-75984
TRENDnet--TEW-WLC100	A vulnerability was detected in TRENDnet TEW-WLC100 1v2.07b01. Affected by this issue is the function FUN_0040da4c of the file /usr/nginx/sbin/nginx of the component HTTP Header Handler. The manipulation of the argument Server results in stack-based buffer overflow. The attack may be launched remotely. The exploit is now public and may be used.	2026-08-18	10	CVE-2026-75784
TRENDnet--TEW-WLC100P	A security vulnerability has been detected in TRENDnet TEW-WLC100P 12.07b01. Affected by this vulnerability is an unknown functionality of the file /sbin/netifd of the component DHCP blobmsg Handler. The manipulation leads to stack-based buffer overflow. The attack must be carried out from within the local network. The exploit has been disclosed publicly and may be used.	2026-08-18	9.6	CVE-2026-75783
TRENDnet--TV-IP751WIC	A flaw has been found in TRENDnet TV-IP751WIC 11.03.03. This vulnerability affects the function SystemNetworkChanged/SystemDDNSChanged/SystemEmailChanged/SystemFTPC changed/websCheckRealm/FUN_00432574/FUN_0043372C of the component alphapd. Executing a manipulation can lead to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been published and may be used.	2026-08-18	9.9	CVE-2026-75877
TRENDnet--TV-IP751WIC	A security flaw has been discovered in TRENDnet TV-IP751WIC 11.03.03. Affected by this issue is some unknown functionality of the file /cgi-bin/admin/set_time.cgi of the component alphapd. The manipulation of the argument Currenttime results in stack-based buffer overflow. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-08-19	9.9	CVE-2026-76584
TRENDnet--TV-IP751WIC	A vulnerability was identified in TRENDnet TV-IP751WIC 11.03.03. Affected by this vulnerability is an unknown functionality of the file /cgi-bin/admin/set_time.cgi of the component alphapd. The manipulation leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	2026-08-19	7.4	CVE-2026-76583
TriliumNext--Trilium	Trilium Notes is a cross-platform, hierarchical note taking application focused on building large personal knowledge bases. Prior to 0.103.0, the #iconClass label value is returned raw by getNotelcon() and inserted without HTML attribute encoding into class attributes in apps/client/src/widgets/quick_search.ts and apps/client/src/services/note_autocomplete.ts, allowing a stored payload to execute automatically when a victim opens a new tab or uses Ctrl+J and, because Electron enables nodeIntegration and disables contextIsolation, run operating-system commands as the victim. This issue is fixed in version 0.103.0.	2026-08-18	8.3	CVE-2026-45733
TrueConf--TrueConf Server	A remote unauthorized attacker with network access via port 4307/TCP to the TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier could execute an arbitrary script by calling an undocumented function.	2026-08-19	9.8	CVE-2026-72529
TrueConf--TrueConf Server	A remote unauthorized attacker with network access via port 4307/TCP to the TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier could use a specially crafted script to break out of the isolated environment and execute arbitrary code on the host system.	2026-08-19	9	CVE-2026-72530
truelockmc--streambert	Streambert is a cross-platform Electron Desktop App to stream and download video content. Prior to 2.5.0, the downloadSubtitleFile utility in src/ipc/downloads.js, reached through the run-download IPC channel, accepts a renderer-supplied subtitle url using the file: URI scheme and passes its decoded pathname to fs.copyFileSync. The renderer also controls downloadPath, which determines the destination path. A compromised renderer can therefore copy any file readable by the StreamBERT process into an attacker-chosen writable location,	2026-08-18	8.8	CVE-2026-52872

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exposing sensitive local data, and can overwrite existing writable files. This vulnerability is fixed in 2.5.0.			
truelockmc--streambert	Streambert is a cross-platform Electron Desktop App to stream and download video content. Prior to version 2.6.0, the open-path-at-time IPC handler in src/ipc/player.js accepts a renderer-controlled filePath without validating its type or location. If the mpv or VLC launch attempts are skipped or fail, the handler passes filePath to Electron's shell.openPath. A compromised renderer can provide the path of a local executable, script, shortcut, or other file with an executing default handler, causing the operating system to launch it with the privileges of the StreamBERT process and enabling escape from the renderer sandbox. This issue is fixed in version 2.6.0.	2026-08-18	8.8	CVE-2026-52876
truelockmc--streambert	Streambert is a cross-platform Electron Desktop App to stream and download video content. Prior to version 2.6.0, the open-external IPC handler in src/ipc/downloads.js passes a renderer-supplied url directly to Electron's shell.openExternal without validating its protocol. A compromised renderer can submit file: URIs or operating-system-specific custom schemes, causing the host to open local files, access remote resources through registered handlers, or launch scripts and applications supported by those handlers. This issue is fixed in version 2.6.0.	2026-08-18	8.3	CVE-2026-52877
Tyche Softwares.--Abandoned Cart Pro for WooCommerce	Unauthenticated Privilege Escalation in Abandoned Cart Pro for WooCommerce <= 10.4.0 versions.	2026-08-20	9.8	CVE-2026-66682
typemill--typemill	Typemill before 2.26.0 contains an authorization bypass vulnerability in the media file download route that allows unauthenticated attackers to access restricted files by submitting path-equivalent URL variants. Attackers can substitute normalized path forms such as dot-slash prefixes, double slashes, or percent-encoded sequences to pass role-based restriction checks while the filesystem resolves the request to the protected file, enabling unauthorized file download without credentials.	2026-08-17	7.5	CVE-2026-71518
Tyrrrz--DiscordChatExporter	DiscordChatExporter saves Discord chat logs to a file. Prior to 2.47.2, HTML exports generated with markdown formatting disabled pass attacker-controlled content through FormatMarkdownAsync and FormatEmbedMarkdownAsync in DiscordChatExporter.Core/Exporting/MessageGroupTemplate.cshtml and render it without HTML entity encoding. The affected fields include message.Content, message.ForwardedMessage.Content, message.ReferencedMessage.Content, embed.Title, embed.Description, field.Name, and field.Value. A Discord webhook or bot can store a script payload in these fields, and the payload executes when a user exports the channel with markdown formatting disabled and opens the resulting HTML, allowing the script to read the export or alter its displayed content. This issue is fixed in version 2.47.2.	2026-08-21	8.2	CVE-2026-54682
uber--kraken	Kraken agents fail to verify peer-to-peer downloaded blobs against their requested SHA-256 digest before committing to the content-addressable cache, relying only on CRC32 checksums for piece validation. Attackers on the agent-to-agent path or malicious peers can supply substituted content with forged CRC32 corrections that passes per-piece checks, poisoning the cache with attacker-chosen container image layers or manifests that are re-seeded and executed by other hosts.	2026-08-18	9	CVE-2026-75625
udecode--plate	Plate is a rich-text editor with AI and shadcn/ui. Prior to 53.3.2, @platejs/docx-io fetches remote image URLs while converting attacker-controlled HTML through htmlToDocxBlob in a server-side or privileged environment. The converter can make requests to internal network resources and include the fetched image bytes in the generated DOCX, allowing server-side request forgery with response disclosure. Applications can also incur resource consumption from attacker-selected remote responses. This issue is fixed in version 53.3.2.	2026-08-20	8.2	CVE-2026-65842
Ultimate Dashboard--Ultimate Dashboard	Unauthenticated Cross Site Scripting (XSS) in Ultimate Dashboard <= 3.11.2 versions.	2026-08-18	7.1	CVE-2026-66621
UNITRONIX--BetterDesk	BetterDesk is a remote desktop management solution. BetterDesk versions through 2.3.0 improperly invalidate deleted device identities, allowing an unauthenticated client to replay or spoof a device ID and bypass registration controls. Version 3.0.0-alpha contains a patch. No known workarounds are available.	2026-08-18	7.7	CVE-2026-50575

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Unleash--unleash	Unleash is an open-source feature management platform. Prior to 7.5.2, 7.6.5, and 8.0.2, the shared OpenAPI validation error path in <code>src/lib/error/bad-data-error.ts</code> passes a raw request value from <code>lodash.get</code> to <code>JSON.stringify</code> in <code>genericErrorMessage</code> and <code>fromOpenApiValidationErrors</code> without guarding stack exhaustion. An unauthenticated attacker can send a roughly 10 KB JSON value nested thousands of levels deep to <code>POST /edge/validate</code> , <code>POST /edge/issue-token</code> , or another OpenAPI-validated endpoint, causing <code>RangeError: Maximum call stack size exceeded</code> in <code>openAPIValidationMiddleware</code> and terminating the Node process because no <code>uncaughtException</code> handler recovers it. Replaying the request can sustain a complete service outage. This issue is fixed in versions 7.5.2, 7.6.5, and 8.0.2.	2026-08-21	7.5	CVE-2026-63462
Unstructured-IO--unstructured	The unstructured library provides open-source components for ingesting and pre-processing images and text documents, such as PDFs, HTML, Word docs, and many more. From 0.4.7 until 0.24.0, the <code>url</code> argument of <code>partition</code> , <code>partition_html</code> , and <code>partition_md</code> is fetched without host validation in <code>unstructured/partition/auto.py</code> , <code>unstructured/partition/html/partition.py</code> , and <code>unstructured/partition/md.py</code> . An attacker who controls that URL can make a server-side ingestion service request loopback addresses, internal HTTP services, or cloud metadata endpoints through direct targets, redirects, or DNS rebinding. The response body is returned as Element text, allowing internal response disclosure, and side-effecting GET endpoints may also be triggered. This issue is fixed in version 0.24.0.	2026-08-20	9.3	CVE-2026-71428
Uptash--Context7	Context7 through 2.1.2 contains a prompt injection vulnerability that allows attackers to execute malicious instructions in connected AI coding agents by injecting unsanitized content through the Custom AI Instructions feature served via the MCP server. Attackers can poison the custom instructions to exfiltrate credentials from environment files to an attacker-controlled service and perform destructive file deletion on the victim's machine when the agent makes a routine library documentation request.	2026-08-18	9	CVE-2026-75130
UTT--HiPER 1200GW	A weakness has been identified in UTT HiPER 1200GW up to 2.5.3-170306. Affected is the function <code>strcpy</code> of the file <code>/goform/formGroupConfig</code> . Executing a manipulation of the argument <code>timestart</code> can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2026-08-19	9.9	CVE-2026-76003
UTT--HiPER 1250GW	A security vulnerability has been detected in UTT HiPER 1250GW up to 3.2.7-210907-180535. Affected by this vulnerability is the function <code>strcpy</code> of the file <code>/goform/aspApBasicConfigUrcp</code> of the component HTTP Handler. The manipulation of the argument <code>pvid</code> leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2026-08-19	9.9	CVE-2026-76004
uxper--Golo Framework	Unauthenticated Local File Inclusion in Golo Framework < 1.7.5 versions.	2026-08-20	8.1	CVE-2026-28150
valkey-io--valkey	Valkey is a distributed key-value database. Prior to 7.2.14, 8.0.10, 8.1.9, 9.0.5, and 9.1.1, Valkey's <code>RESTORE</code> command accepts a malformed RDB stream payload that assigns one Pending Entry List NACK to multiple consumers during stream consumer-group deserialization, causing a use-after-free when one consumer is deleted while another still references the shared NACK and potentially allowing remote code execution. This issue is fixed in versions 7.2.14, 8.0.10, 8.1.9, 9.0.5, and 9.1.1.	2026-08-18	8.8	CVE-2026-63639
valkey-io--valkey	Valkey is a distributed key-value database. Prior to 7.2.14, 8.0.10, 8.1.9, 9.0.5, and 9.1.1, Valkey's <code>tlsProcessPendingData</code> function iterates <code>pending_list</code> while an authenticated client can trigger <code>CLIENT KILL</code> , causing <code>connTLSClose</code> to delete the iterator's cached next node and producing a use-after-free that can crash the server or potentially allow remote code execution when TLS is enabled. This issue is fixed in versions 7.2.14, 8.0.10, 8.1.9, 9.0.5, and 9.1.1.	2026-08-18	7.5	CVE-2026-56684
vas3k--TaxHacker	A vulnerability was identified in vas3k TaxHacker up to 0.8.2. The affected element is the function <code>envSchema.parse</code> of the file <code>lib/config.ts</code> of the component JWT Secret Handler. The manipulation of the argument <code>BETTER_AUTH_SECRET</code> leads to hard-coded credentials. The attack can be initiated remotely. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-23	7.3	CVE-2026-78062
VaultDweller--Leyka	Subscriber Broken Authentication in Leyka <= 3.32.3 versions.	2026-08-20	7.6	CVE-2026-66677
verbb--formie	Formie is a Craft CMS plugin for creating forms. Prior to 3.1.27, Formie can pass request-derived Hidden field defaults such as HTTP User Agent, Referer URL, Current URL, Current URL without Query String, Query Parameter, and Cookie Value to Craft's Twig rendering layer during front-end form rendering. An	2026-08-19	9.8	CVE-2026-52889

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated attacker can place Twig syntax in one of these request-controlled inputs when a public form contains an affected Hidden field. Hidden::getFrontEndInputOptions() then assigns the value to defaultValue and calls renderString, causing server-side template evaluation rather than treating the request data as a plain string. Depending on the Craft site configuration and available Twig capabilities, exploitation can disclose sensitive information, modify application state, or achieve remote code execution. This issue is fixed in version 3.1.27.			
veronalabs--WP Statistics Simple, privacy-friendly Google Analytics alternative	The WP Statistics - Simple, privacy-friendly Google Analytics alternative plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'utm_campaign' parameter in all versions up to, and including, 14.16.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload can be planted without authentication via the public /wp-statistics/v2/hit REST endpoint, because the required signature is exposed on the public homepage and a base64-encoded page_uri POST parameter overrides the previously sanitized REQUEST_URI, allowing the malicious utm_campaign value to bypass sanitization and be stored in the database.	2026-08-19	7.2	CVE-2026-15780
vim--vim	A flaw was found in Vim's netrw plugin. A crafted filename containing quote characters and expression fragments can break out of the quoted context during mark/unmark operations, allowing arbitrary Vimscript execution. This can be leveraged to run shell commands with the privileges of the user running Vim.	2026-08-19	7.8	CVE-2026-43961
Vladimir Prelovac--Theme Test Drive	Unauthenticated Local File Inclusion in Theme Test Drive <= 2.9.1 versions.	2026-08-18	8.1	CVE-2026-32464
Volcengine--OpenViking	OpenViking before 0.3.4 contains a server-side request forgery vulnerability that allows authenticated low-privilege attackers to access internal network services by submitting arbitrary URLs to the resources API endpoint. Attackers can POST a crafted URL to /api/v1/resources, causing the server to issue outbound HEAD and GET requests with redirects enabled to loopback, RFC 1918, link-local, or cloud metadata addresses, then read back responses through normal content APIs to enumerate and interact with internal services.	2026-08-21	8.5	CVE-2026-22681
Wasilyi Strecker--Contest Gallery	Unauthenticated Cross Site Scripting (XSS) in Contest Gallery <= 30.0.5 versions.	2026-08-19	7.1	CVE-2026-61986
Wavlink--WN531P3	A vulnerability was determined in Wavlink WN531P3 and WN535M1 V250922. Affected by this vulnerability is the function strcpy of the file /etc/lighttpd/www/cgi-bin/export_pingortrace.cgi of the component Export Pingortrace CGI. Executing a manipulation of the argument HTTP_COOKIE can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	2026-08-17	10	CVE-2026-74843
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.0.0 until 4.14.6 and 5.0.0-beta3, cluster.unmerge_info() in framework/wazuh/core/cluster/cluster.py constructs paths from peer-controlled merge_type and name values in a merged synchronization archive. process_files_from_worker() in framework/wazuh/core/cluster/master.py does not adequately confine the resulting path to the declared cluster item directory. A cluster peer holding the shared Fernet key can use traversal in files_metadata.json or a merged-file header to write files such as /var/ossec/etc/ossec.conf. Replacing ossec.conf can configure root-executed commands and lead to code execution when Wazuh services reload. This issue is fixed in versions 4.14.6 and 5.0.0-beta3.	2026-08-19	9.1	CVE-2026-48024
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.0.0 until 4.14.6 and 5.0.0-beta3, DistributedAPI.send_tmp_file() in framework/wazuh/core/cluster/dapi/dapi.py joins an attacker-controlled tmp_file value to WAZUH_PATH without canonicalization or confinement. A cluster peer holding the shared Fernet key can use traversal or an absolute path to make the master return any readable file over the cluster channel. Reading /var/ossec/api/configuration/security/private_key.pem allows the peer to forge administrator REST API tokens offline and then exercise administrative privileges without creating an account. This issue is fixed in versions 4.14.6 and 5.0.0-beta3.	2026-08-19	9.1	CVE-2026-48162
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.3.0 until 4.14.6 and 5.0.0-beta3, the non-merged branch of process_files_from_worker() in framework/wazuh/core/cluster/master.py trusts a peer-controlled file_path key from files_metadata.json. The destination is joined to	2026-08-19	9.1	CVE-2026-49441

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WAZUH_PATH without proving that it remains inside the directory selected by cluster_item_key. A cluster peer holding the shared Fernet key can upload a crafted extra-valid archive and overwrite security-sensitive files such as /var/ossec/etc/ossec.conf. Replacing ossec.conf can configure root-executed commands and lead to code execution after a service reload. This issue is fixed in versions 4.14.6 and 5.0.0-beta3.			
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.9.0 until 4.10.4 and 4.14.6, PUT /security/users/{user_id} in api/api/controllers/security_controller.py passes request.get("user") instead of request.context['token_info']['sub'] as current_user. remove_nones_to_dict() removes the resulting None value, so the reserved-account protection in framework/wazuh/security.py cannot verify who is making the request. An authenticated user with the users_admin role can overwrite the password of protected administrator accounts with user IDs at or below 99, including the wazuh superuser, and gain full administrative control. This issue is fixed in versions 4.10.4 and 4.14.6.	2026-08-19	8.2	CVE-2026-41424
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.0.0 until 4.14.6 and 5.0.0-beta2, AffectedItemsWazuhResult.merge() in framework/wazuh/core/results.py trusts the sort_casting field in a cluster worker's JSON response. During a distributed API merge, attacker-controlled type names are resolved through Python builtins without an allowlist. A compromised worker can set sort_casting to exec and place Python source in affected_items, causing the master to execute the payload as root when responses from multiple nodes are merged. This issue is fixed in versions 4.14.6 and 5.0.0-beta2.	2026-08-19	8.4	CVE-2026-44901
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.5.0 until 4.14.6 and 5.0.0-beta2, compare_wazuh_versions() in src/shared/version_op.c copies the attacker-controlled enrollment V: field into a 10-byte stack buffer with strncpy() but does not explicitly terminate the buffer. The function is reachable before authentication through wazuh-authd on TCP port 1515 when anonymous TLS enrollment is enabled. A version string of at least nine non-null bytes can cause strchr() and strtok() to read beyond ver2 and can make strtok() write a null byte into adjacent stack memory, allowing a remote denial of service. This issue is fixed in versions 4.14.6 and 5.0.0-beta2.	2026-08-19	7.5	CVE-2026-45798
Wazuh--wazuh-manager	Wazuh 4.0.0 before 4.14.6 contains a path traversal vulnerability that allows unauthenticated remote attackers to cause denial of service by enrolling an agent with a dot-sequence name such as ".." through the enrollment port. Attackers exploit insufficient validation in OS_IsValidName() and unsafe path concatenation in delete_diff() to resolve the traversal to the parent queue directory, causing its subdirectories to be removed and stopping all Wazuh services requiring manual recovery.	2026-08-18	7.1	CVE-2026-74038
wbolt.com--Online Contact Widget	Unauthenticated Broken Access Control in Online Contact Widget <= 1.3.0 versions.	2026-08-18	7.5	CVE-2026-32472
Webnus Inc.--Modern Events Calendar	Unauthenticated SQL Injection in Modern Events Calendar < 7.35.0 versions.	2026-08-18	9.3	CVE-2026-73339
weDevs--Subscribe2	Unauthenticated Cross Site Scripting (XSS) in Subscribe2 <= 10.46 versions.	2026-08-18	7.1	CVE-2026-73393
weechat--weechat	WeeChat (Wee Enhanced Environment for Chat) is a free chat client. In versions 0.3.1 through 4.9.0, the WeeChat relay authentication uses non-constant-time string comparison functions (weechat_strcasecmp and strcmp) to verify password hashes and plaintext passwords. An attacker can exploit timing differences to extract the server-computed hash character by character, then authenticate using the correct hash without knowing the password. Version 4.9.1 fixes the issue.	2026-08-21	7.4	CVE-2026-53525
wekan--wekan	Wekan is open source kanban built with Meteor. From 8.36 until 9.74, the outgoing webhook Integration URL validator in models/integrations.js checked only the literal URL.hostname against regular expressions, so DNS names such as 169-254-169-254.nip.io passed that first-line check. The delivery path's fetchSafe guard already blocked the reported IPv4 destination, but its separate IPv4-only resolver and duplicated blocklist created inconsistent all-address-family enforcement and drift risk between input-time and connection-time validation. Version 9.74 makes server/lib/ssrfGuard.js resolve all addresses with `dns.lookup({ all: true })`, validate every result through the shared isIpBlocked logic, pin the connection, and block redirects. This issue is fixed in version 9.74.	2026-08-19	8.5	CVE-2026-68558

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wekan--wekan	Wekan is open source kanban built with Meteor. Prior to 9.89, the second Boards.allow({ update }) rule in server/permissions/boards.js called canUpdateBoardSort in server/lib/utls.js, which authorized any board member whenever fieldNames included sort. Because Meteor combines allow rules with OR semantics and applies the complete modifier, a comment-only or read-only member could send one Boards.update with \$set values for sort, members, permission, and title, make themselves the sole board administrator, expose a private board, and evict the legitimate owner; the last-admin deny rule inspected only \$pull and did not block a wholesale \$set of members. Version 9.89 requires sort to be the only modified field and rejects \$set member arrays that remove the last active administrator. This issue is fixed in version 9.89.	2026-08-19	8.8	CVE-2026-68561
wekan--wekan	Wekan is open source kanban built with Meteor. Prior to 9.90, isFileValid() in models/fileValidation.js used the Unix file command for content-based MIME detection, but detectMimeFromFile() silently returned undefined when that binary was unavailable and the validation fell back to the attacker-controlled fileObj.type supplied through server/routes/attachmentApi.js. On deployments with WITH_API=true and no file binary, an authenticated board member could label HTML containing JavaScript as image/png, bypass the dangerous MIME check, and store active content under the Wekan origin for execution when another user opened it. Version 9.90 adds looksLikeDangerousMarkup() to inspect file bytes and force dangerous-content scanning when MIME detection is unavailable. This issue is fixed in version 9.90.	2026-08-19	8.7	CVE-2026-68899
wekan--wekan	Wekan is open source kanban built with Meteor. From 8.72 until 10.23, addBoardHTMLToZip() in client/lib/exportHTML.js read a card title and body through textContent, which decoded entity-encoded markup, and then interpolated titleText and allText into content.innerHTML in the exported index.html. A board member could store an entity-encoded event-handler payload in a card title that remained inert on the live board but was reparsed and executed when a recipient clicked the card in the downloaded HTML export, allowing the script to read and transmit all board data contained in that export, including content added after the attacker's membership was removed. Version 10.23 builds the modal with DOM nodes and assigns untrusted values through textContent. This issue is fixed in version 10.23.	2026-08-19	7.6	CVE-2026-68900
westguard--WS Form LITE Drag & Drop Contact Form Builder	The WS Form LITE - Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.10.80 via deserialization of untrusted input from form submission meta values. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	2026-08-22	9.8	CVE-2026-4703
Wireshark Foundation--Wireshark	C12.22 protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	8.1	CVE-2026-76886
Wireshark Foundation--Wireshark	C12.22 protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	7.5	CVE-2026-76879
Wireshark Foundation--Wireshark	RRC protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	7.5	CVE-2026-76880
Wireshark Foundation--Wireshark	X.509IF protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	7.5	CVE-2026-76928
wordplus--BP Better Messages	Unauthenticated Cross Site Scripting (XSS) in BP Better Messages <= 2.15.22 versions.	2026-08-18	7.1	CVE-2026-32547
WordPress.com--eShipper Commerce	Subscriber SQL Injection in eShipper Commerce <= 2.16.13 versions.	2026-08-20	8.5	CVE-2026-74013
WP Grids--Convert Pro	Unauthenticated Cross Site Scripting (XSS) in Convert Pro <= 1.0.1 versions.	2026-08-18	7.1	CVE-2026-68567
wp.insider--Affiliates Manager	Unauthenticated SQL Injection in Affiliates Manager <= 2.9.53 versions.	2026-08-18	9.3	CVE-2026-73355

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wp.insider--Affiliates Manager	Unauthenticated Cross Site Scripting (XSS) in Affiliates Manager <= 2.9.53 versions.	2026-08-18	7.1	CVE-2026-73358
wpdesk--Flexible Subscriptions	Customer PHP Object Injection in Flexible Subscriptions <= 1.8.1 versions.	2026-08-19	9.8	CVE-2026-73364
WPDeveloper--Templately	Unauthenticated Cross Site Scripting (XSS) in Templately <= 3.7.1 versions.	2026-08-18	7.1	CVE-2026-66667
WPEverest--User Registration & Membership Pro	Unauthenticated Broken Authentication in User Registration & Membership Pro <= 5.4.5 versions.	2026-08-20	9.8	CVE-2026-74001
WPExperts--Gravity Forms Bookings premium	Subscriber SQL Injection in Gravity Forms Bookings premium <= 2.1 versions.	2026-08-18	8.5	CVE-2026-32466
wpfeedback--Atarim AI Agency for WordPress: Edit Pages, Fix Code, Update Plugins, SEO & Client Feedback	The Atarim - AI Agency for WordPress: Edit Pages, Fix Code, Update Plugins, SEO & Client Feedback plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the AVCF_Abilities_Media::register (replace-media-file execute_callback) function in all versions up to, and including, 5.1.1. This makes it possible for authenticated attackers, with author-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). This is exploitable by first using the atarim/update-post-field ability to overwrite the _wp_attached_file meta of an attacker-owned attachment with a directory-traversal path, then invoking atarim/replace-media-file to cause get_attached_file() to resolve and unlink the targeted file.	2026-08-19	8.1	CVE-2026-19942
WPForms--WPForms Pro	The WPForms Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Single Line Text and Paragraph Text Field Values in all versions up to, and including, 2.0.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit relies on the plugin's own wp_kses_allowed_html filter widening the 'post' allowlist to permit iframe elements with a data-src attribute, which is not on WordPress's URI-attribute sanitization list, allowing a javascript: URI stored in data-src to survive kses processing and subsequently be promoted to a live src attribute by the bundled admin script view-entry.min.js.	2026-08-21	7.2	CVE-2026-18409
WPManageNinja--Fluent Forms Pro Add On Pack	Unauthenticated Cross Site Scripting (XSS) in Fluent Forms Pro Add On Pack < 6.2.12 versions.	2026-08-18	7.1	CVE-2026-66633
WPMU DEV--Forminator	Unauthenticated PHP Object Injection in Forminator <= 1.57.0 versions.	2026-08-20	9.8	CVE-2026-66583
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.56.1 via the handle_file_upload function. This is due to insufficient file type validation in handle_file_upload, where the dangerous-extension blacklist performs exact-key matching that is bypassed by pipe-alternative MIME type keys, combined with a public submission handler that trusts attacker-controlled upload field configuration injected via a forged Select field value. This makes it possible for unauthenticated attackers to upload files that may be executable, which makes remote code execution possible.	2026-08-18	9.8	CVE-2026-15748
wpo-HR--NGG Smart Image Search	Unauthenticated SQL Injection in NGG Smart Image Search < 4.0.0 versions.	2026-08-19	9.3	CVE-2026-73185
WPPOOL--FormyChat	Unauthenticated Broken Access Control in FormyChat <= 2.15.7 versions.	2026-08-18	7.5	CVE-2026-28571
wpWax--Templatic	Contributor Arbitrary File Upload in Templatic <= 0.2.5 versions.	2026-08-18	9.9	CVE-2026-32474
WPZOOM--Recipe Card Blocks for Gutenberg & Elementor	Unauthenticated Cross Site Scripting (XSS) in Recipe Card Blocks for Gutenberg & Elementor <= 3.4.18 versions.	2026-08-18	7.1	CVE-2026-73361
WWBN--AVideo	AVideo through commit 9c39d8c8 contains an authentication bypass vulnerability where deduplicateByEncoderQueueId() returns video_id_hash credentials for any video by encoder_queue_id without ownership verification, and useVideoHashOrLogin() converts this hash into passwordless login as the video owner. Attackers with upload permission can retrieve an administrator's video_id_hash by omitting the videos_id parameter, then use that hash in an unauthenticated request to gain administrative session access and modify system configuration.	2026-08-22	8.8	CVE-2026-59808

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WWBN--AVideo	WWBN AVideo through commit 9c39d8c8 contains a cross-site request forgery vulnerability in the releaseVideoNow.json.php endpoint that lacks authenticity checks and accepts GET requests. Attackers can craft a malicious cross-site GET request carrying an administrator's session cookie to permanently publish any embargoed video by manipulating the videos_id parameter.	2026-08-22	7.1	CVE-2026-58003
WWBN--AVideo	WWBN AVideo through commit 9c39d8c8 contains an authorization bypass vulnerability where getToken() creates tokens without binding to user identity or purpose, and plugin/Gallery/view/sections.php issues valid tokens to unauthenticated visitors. Attackers can retrieve a token from the Gallery endpoint and use it to bypass authorization checks in other subsystems like view/hls.php to access restricted video content.	2026-08-22	7.5	CVE-2026-59256
xorbitsai--inference	Xinference is an inference API for running open-source, speech, and multimodal models. In 2.5.0 and earlier, Xinference passes attacker-influenced Llama3 tool-call output to eval() in xinference/model/llm/tool_parsers/llama3_tool_parser.py and xinference/model/llm/utlis.py. Requests to /v1/chat/completions with a tools field flow through xinference/api/restful_api.py, xinference/model/llm/transformers/core.py, handle_chat_result_non_streaming(), and _post_process_completion() before extract_tool_calls() or _eval_llama3_chat_arguments() evaluates the model-generated Python expression. An unauthenticated remote attacker can influence that output through a crafted prompt and execute commands in the Xinference server process context. This issue is fixed in version 2.7.0.	2026-08-21	10	CVE-2026-61539
YITH--YITH WooCommerce Membership Premium	Subscriber SQL Injection in YITH WooCommerce Membership Premium <= 2.33.0 versions.	2026-08-19	8.5	CVE-2026-32552
YOURLS--YOURLS	YOURLS is a self-hosted, customizable URL shortener written in PHP. From 1.5.1 until 1.10.4, YOURLS stores the HTTP Referer header through yourls_get_referrer(), yourls_sanitize_url_safe(), and yourls_log_redirect(), then aggregates the value in yourls-infos.php and passes the derived domain through yourls_get_domain(), yourls_stats_pie(), and yourls_google_array_to_data_table(). The chart builder concatenates labels into inline JavaScript without JavaScript-string escaping, so an unauthenticated attacker can poison the statistics of an existing short URL with a crafted referrer. When an administrator or public stats-page viewer opens the affected statistics page, attacker-controlled JavaScript executes in the YOURLS origin and can access admin-visible data, the API signature token, and privileged same-origin actions. This issue is fixed in version 1.10.4.	2026-08-21	8.2	CVE-2026-63135
Youzify--Youzify	Unauthenticated Deserialization of untrusted data in Youzify <= 1.3.7 versions.	2026-08-18	9.8	CVE-2026-73397
zanllp--infinite-image-browsing	is_path_trusted in scripts/iib/api.py compares the requested path against each allowed parent directory with path.startswith(parent_path), without appending a path separator. A directory whose name merely begins with an allowed path therefore satisfies the comparison, so where /data/images is allowed a request for /data/images_private/secret.txt is treated as trusted and served by FileResponse, disclosing files the confinement was meant to exclude. Whether the check applies depends on get_enable_access_control in scripts/iib/tool.py: it returns true when IIB_ACCESS_CONTROL is set to enable, false when set to disable, and otherwise true when the host Stable Diffusion WebUI was started with share, ngrok, listen or server_name, falling back to false. Confinement is therefore active in the network-exposed WebUI deployments that rely on it, while a standalone run with no such option serves every readable file regardless of this flaw. The fix compares against parent_path joined with os.sep.	2026-08-21	7.5	CVE-2026-77814
zanllp--infinite-image-browsing	to_abs_path in scripts/iib/tool.py normalised the requested path with os.path.normpath, which collapses dot segments but does not resolve symbolic links. A symlink placed inside a scanned directory therefore satisfies the containment comparison performed by is_path_trusted in scripts/iib/api.py while pointing outside that directory, and FileResponse follows the link when serving the response, so a link created in an image directory and targeting a file such as /etc/passwd discloses that file. Whether the check applies depends on get_enable_access_control in scripts/iib/tool.py: it returns true when IIB_ACCESS_CONTROL is set to enable, false when set to disable, and otherwise true when the host Stable Diffusion WebUI was started with share, ngrok, listen or server_name, falling back to false. Confinement is therefore active in the network-exposed WebUI deployments that rely on it, while a standalone run with no such	2026-08-21	7.5	CVE-2026-77815

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	option serves every readable file regardless of this flaw. The fix resolves the path with os.path.realpath.			
ZcashFoundation--zebra	ZEBRA is a Zcash node written entirely in Rust. Prior to 4.5.0, an unauthenticated IPv4 peer can deterministically terminate a synced Zebra node using the default Linux dual-stack listener configuration. The handshake path canonicalized an IPv4-mapped IPv6 PeerSocketAddr such as ::ffff:127.0.0.1 to plain IPv4 before storing it through MetaAddr::new_connected, but the mempool misbehavior path forwarded the raw transient address to MetaAddrChange::UpdateMisbehavior. In zebra-network/src/meta_addr.rs, apply_to_meta_addr then compared the canonical address-book entry with the raw update address and reached its unexpected address mismatch assertion. After the misbehavior batch flush, panic equals abort terminated zebra; the peer only needed to complete a P2P handshake and advertise an invalid mempool transaction. This issue is fixed in version 4.5.0.	2026-08-18	7.5	CVE-2026-52829
ZealousWeb--Track Geolocation Of Users Using Contact Form 7	Unauthenticated Sensitive Data Exposure in Track Geolocation Of Users Using Contact Form 7 <= 3.0.2 versions.	2026-08-19	7.5	CVE-2026-73386
zephyrproject--zephyr	The HL7800 cellular modem driver's +CGCONTRDP: response handler on_cmd_atcmdinfo_ipaddr() in drivers/modem/vendor_standalone/hl7800.c parses the PDP-context dynamic parameters (local address, subnet mask, gateway, and DNS servers) that the cellular network assigns to the device. The response is linearized into a 256-byte stack buffer, after which each address field length is computed from comma/. delimiter positions in the network-supplied data and used directly as the length argument to strncpy() into the fixed 64-byte stack buffer temp_addr_str (and the 16-byte iface_ctx.dns_v4_string). Because the field length is derived from attacker-controlled delimiter positions and was not bounded against the destination buffer, a single field can be far larger than 64 bytes. A malicious or impersonated cellular network (for example a rogue base station) can return a crafted +CGCONTRDP response with an overlong address field, causing strncpy() to write past temp_addr_str on the modem worker thread's stack, plus an out-of-bounds NUL write at temp_addr_str[addr_len]. No device-side privileges or user interaction are required: the device itself issues the AT+CGCONTRDP=1 query during normal network attach and parses whatever the network returns. The overflow corrupts adjacent stack memory in supervisor context, yielding at minimum a remotely triggerable crash and potentially control-flow hijacking on targets without stack protection. The fix bounds every field length against its destination buffer (temp_addr_str and dns_v4_string) before each copy, rejecting overlong fields.	2026-08-19	8.8	CVE-2026-12522
zephyrproject--zephyr	The IPv6 neighbor-discovery code in subsys/net/ip/ipv6_nbr.c processes the 6LoWPAN Context Option (6CO, RFC 6775) carried inside ICMPv6 Router Advertisements. In handle_ra_6co() the 8-bit context_len field is taken directly from the packet and was never bounded to the RFC maximum of 128. The function computes context->context_len / 8 and then performs memset(context->prefix + context_len, 0, sizeof(context->prefix) - context_len), where context->prefix is a fixed 16-byte array. With context_len between 136 and 255 (and the option length field set to 3, which the pre-fix validation accepts), context_len / 8 evaluates to 17..31, so the memset length 16 - context_len/8 underflows the unsigned size_t argument to roughly SIZE_MAX. This produces an unbounded out-of-bounds memset that zeroes kernel memory well past the 6lo context structure. The defect is reachable from unauthenticated, link-local input: any host on the same link can send a crafted Router Advertisement with a 6CO option. The RA handler validates only the option length field before calling handle_ra_6co(), so a single packet triggers the wild write. The code is compiled when CONFIG_NET_6LO_CONTEXT is enabled. The impact is a reliable remote (adjacent) denial of service via memory corruption, with collateral integrity loss as the memset zeroes contiguous memory before the system faults. Router Advertisements are link-scoped and not forwarded, so the attacker must be on the same link (AV:A). The fix rejects any context_len greater than 128 before the length computation.	2026-08-19	8.1	CVE-2026-12633
zephyrproject--zephyr	The flash_copy() system call is verified by z_vrfy_flash_copy() in drivers/flash/flash_util.c. On builds with CONFIG_USERSPACE enabled, this handler is the kernel-side trust boundary for a user-mode caller. Prior to the fix it validated only the output buffer (K_SYSCALL_MEMORY_WRITE) and passed the two struct device * arguments, src_dev and dst_dev, directly into the implementation without any object validation - unlike every sibling flash syscall, which guards its device	2026-08-17	8.8	CVE-2026-9771

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pointer with K_SYSCALL_DRIVER_FLASH. A user-mode thread fully controls the values of src_dev/dst_dev and the contents of its own address space. The implementation z_impl_flash_copy() dereferences these pointers and calls through their driver-API function tables (e.g. api->get_parameters(dst_dev), flash_read(src_dev, ...), flash_write(dst_dev, ...)). By supplying a pointer to a forged struct device whose api table contains attacker-chosen function pointers, an unprivileged thread can cause the kernel to call arbitrary code in supervisor mode; passing any arbitrary or invalid address otherwise yields a kernel crash or out-of-bounds read. The result is a local privilege escalation out of the userspace sandbox (with kernel denial-of-service and information disclosure as lesser outcomes). The fix adds K_SYSCALL_DRIVER_FLASH(src_dev, read) and K_SYSCALL_DRIVER_FLASH(dst_dev, write) to z_vrfy_flash_copy(), which verify each device is a registered flash-driver kernel object the calling thread is permitted to use before any dereference, closing the path completely.			
4MOSAn Security Technology-- 4MOSAn GCB Doctor	4MOSAn GCB Doctor developed by 4MOSAn Security Technology has a OS Command Injection vulnerability. Unauthenticated remote attackers can inject malicious commands through an unremoved ADODB test page parameter, thereby executing arbitrary system commands on the server.	2026-08-24	9.8	CVE-2026-78211
4MOSAn Security Technology-- 4MOSAn Management Center	4MOSAn developed by 4MOSAn Security Technology Co., Ltd. has an Arbitrary File Read vulnerability. Unauthenticated remote attackers can exploit a Relative Path Traversal flaw to download arbitrary system files.	2026-08-24	7.5	CVE-2026-78212
A CPT--ACPT (Pro) - Custom Post Types Plugin for WordPress	Subscriber PHP Object Injection in ACPT (Pro) - Custom Post Types Plugin for WordPress <= 2.0.63 versions.	2026-08-24	9.8	CVE-2026-32563
AcademySoftware Foundation-- openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. Versions before 3.2.11, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13 allow a crafted EXR with a nonzero dataWindow.min to make TypedFlatImageChannel::row() return an invalid heap pointer, causing out-of-bounds or use-after-free writes. This occurs when an application writes rows through FlatHalfChannel::row(). Affected consumers are tools, converters, render pipeline components, or image-processing services that accept untrusted EXR files and use FlatHalfChannel::row() on loaded images. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	7.1	CVE-2026-59184
AcademySoftware Foundation-- openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. In versions before 3.2.11, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13, a crafted tiled EXR can trigger a heap out-of-bounds write on 32-bit/ILP32 builds when read through the public TiledRgbaInputFile RGBA API. The file uses a small 40x40 dataWindow but a 65537x65537 tile size. On ILP32, the Array2D<Rgba> tile-conversion buffer size calculation overflows, allocates a much smaller heap buffer, and tile decode writes past that allocation. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	7.1	CVE-2026-59186
AcademySoftware Foundation-- openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. OpenEXR versions 3.3.0 through 3.3.12 and 3.4.0 through 3.4.13 are vulnerable to a heap out-of-bounds write when exrmetrics reads a crafted deep scanline EXR. This occurs with pixel conversion options such as --pixelmode float or --bench because DeepSlice requests FLOAT output while the backing sample buffers are allocated using the input HALF element size. The issue is fixed in versions 3.3.13 and 3.4.14.	2026-08-25	7.1	CVE-2026-59187
AcademySoftware Foundation-- openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. In OpenEXRUtil versions 3.3.0 through 3.3.12 and 3.4.0 through 3.4.12, the documented TypedDeepImageChannel<T>::row() API can return an out-of-bounds pointer when a deep image has a non-zero dataWindow origin, resulting in a heap out-of-bounds read and crash, with potential information disclosure under a controlled heap layout. The flaw arises because ImfDeepImageChannel uses two conflicting coordinate models: at(x, y) uses absolute coordinates (with _base offset by dataWindow.min), while row(r) is documented as 0-based logical access. For a non-zero dataWindow.min, row(0) therefore points outside the _sampleListPointers allocation instead of at the first logical row. This issue is fixed in versions 3.3.13 and 3.4.13.	2026-08-25	7.1	CVE-2026-59189

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image file format, widely used in the motion picture industry. In versions through 3.2.10, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13, the OpenEXRUtil library returns an out-of-bounds pointer from the SampleCountChannel::row() API when a deep image has a non-zero dataWindow origin. The row() accessor is documented as 0-based and computes its address from an internal base that is offset for absolute pixel coordinates, so the two coordinate models conflict whenever dataWindow.min is non-zero. For a deep image whose data window has a large negative vertical origin, row(0) points far outside the allocated sample-count buffer. An application that opens an attacker-controlled deep EXR file and accesses sample counts through row() performs an out-of-bounds read, which can crash the process or, under a controlled heap layout, return adjacent heap memory as sample-count values. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	7.1	CVE-2026-59981
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. OpenEXR versions before 3.2.11, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13 can return an out-of-bounds pointer from TypedDeepImageChannel::row() when a crafted deep EXR has a nonzero dataWindow origin. This vulnerability occurs because the API combines zero-based row access with an absolute-coordinate-adjusted base pointer, allowing a crash or limited information disclosure. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	7.1	CVE-2026-59982
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. Versions 3.3.0 through 3.3.12 and 3.4.0 through 3.4.13 contain a heap buffer overflow in PyOpenEXR triggered by a channel-name key collision between literal and prefixed RGB channels. When separate_channels=false, PyOpenEXR maps each physical channel name through channelNameToRGBA() and coalesces the results into a shared RGB array. A crafted flat scanline EXR that contains both a literal channel such as left and prefixed channels such as left.R, left.G, and left.B causes these names to collide, so the wrapper reuses an undersized two-dimensional NumPy array for the coalesced RGB slices and writes out of bounds when OpenEXR.File(path) decodes the pixels. This issue is fixed in versions 3.3.13 and 3.4.14.	2026-08-25	7.1	CVE-2026-68513
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. In versions before 3.2.11, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13, exrmultiview can write past a heap allocation when it combines two attacker-supplied, individually valid scanline EXR files whose union dataWindow is not aligned to one view's channel subsampling. The utility allocates sampled channel storage using a truncated union_width / xSampling, then reads the sampled input through a Slice based on the misaligned union window, producing a heap out-of-bounds write. The trigger is normal public-tool processing, such as exrmultiview left A.exr right B.exr out.exr with crafted but valid inputs, so this is not solely an API or caller-precondition issue. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	7.1	CVE-2026-68515
ACPT--ACPT (Pro) - Custom Post Types Plugin for WordPress	Unauthenticated Privilege Escalation in ACPT (Pro) - Custom Post Types Plugin for WordPress <= 2.0.63 versions.	2026-08-27	9.8	CVE-2026-32566
ACPT--ACPT (Pro) - Custom Post Types Plugin for WordPress	Subscriber SQL Injection in ACPT (Pro) - Custom Post Types Plugin for WordPress <= 2.0.63 versions.	2026-08-27	8.5	CVE-2026-32564
Addify--Custom User Registration Fields for WooCommerce	The Custom User Registration Fields for WooCommerce plugin for WordPress is vulnerable to Privilege Escalation in versions up to, and including, 2.2.3. This is due to the plugin accepting an attacker-controlled afreg_select_user_role value from the unauthenticated WooCommerce Store API /wc/store/v1/checkout request in the af_reg_checkout_data_to_order_meta_data_block() function, persisting it in order meta, and then passing it directly to WP_User::add_role() in the af_reg_custom_order_processing_function() function (hooked to woocommerce_thankyou) without validating against the plugin's admin-configured allowed role list. This makes it possible for unauthenticated attackers to elevate their privileges to Administrator by creating an account during checkout with a modified JSON body specifying administrator (or any other role slug) as the desired role. Note: The exploit requires the "User Role Selection" setting to be enabled.	2026-08-29	9.8	CVE-2026-15369

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Admidio--admidio	Admidio before 5.0.12 contains a blind SQL injection vulnerability in the relation_type_list parameter of lists_show.php that allows unauthenticated attackers to execute arbitrary SQL queries. Attackers can bypass authentication by providing a dummy UUID in role_list and inject SQL through relation_type_list to extract database contents including password hashes and user credentials.	2026-08-30	7.5	CVE-2026-82655
Admidio--admidio	Admidio before 5.0.12 fails to enforce login-only module restrictions in RSS feed endpoints for forum and announcements modules. Unauthenticated attackers can retrieve forum topics and announcements by sending GET requests to rss/forum.php or rss/announcements.php, disclosing titles, full post text, author names, and timestamps.	2026-08-30	7.5	CVE-2026-82657
Admin By Request (ABR)--Admin By Request (ABR)	An insecure PIN derivation mechanism in ABR allows a low-privileged user to escalate privileges to administrator by communicating over Cross-Process Communication (XPC) while masquerading as an Apple-signed process.	2026-08-26	8.8	CVE-2026-78236
Admin By Request (ABR)--Admin By Request (ABR)	Insufficient input validation in ABR allows a low-privileged user to inject malicious entries into the sudoers file, resulting in persistent root access that remained effective after the ABR session ended.	2026-08-26	7.8	CVE-2026-78237
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-25	10	CVE-2026-76193
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-25	10	CVE-2026-76195
Adobe--Adobe Campaign Classic	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-08-25	10	CVE-2026-76197
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48426
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48427
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48428
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48430
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48431
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48432
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48433
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-71564

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler versions 5.1.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-27	7.8	CVE-2026-34674
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48417
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48418
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48419
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48420
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48421
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48422
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48423
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48424
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-48425
Adobe--Adobe Substance 3D Sampler	Substance3D - Sampler is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-71382
Adobe--Adobe XD	Adobe XD is affected by a Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-71399
Adobe--C2PA Tool	CAI Content Credentials is affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-25	7.5	CVE-2026-71360
Adobe--C2PA Tool	CAI Content Credentials is affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-25	7.5	CVE-2026-71442
Adobe--C2PA Tool	CAI Content Credentials is affected by an Improper Input Validation vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-25	7.5	CVE-2026-71443
Adobe--Substance3D - Painter	Substance3D - Painter is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user.	2026-08-25	7.8	CVE-2026-75749

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
Adobe--Substance3D - Painter	Substance3D - Painter is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-75750
Adobe--Substance3D - Painter	Substance3D - Painter is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-75766
Adobe--Substance3D - Painter	Substance3D - Painter is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-75767
Adobe--Substance3D - Painter	Substance3D - Painter is affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-75768
Adobe--Substance3D - Painter	Substance3D - Painter is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-75769
Adobe--Substance3D - Painter	Substance3D - Painter is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	7.8	CVE-2026-75770
airbytehq--airbyte-platform	Airbyte Platform resolves the workspace used for its authorization decision from a field the caller supplies. AuthorizationServerHandler copies recognised identifiers out of the raw JSON request body into X-Airbyte-* headers, and AuthenticationHeaderResolver.resolveWorkspace consults X-Airbyte-Workspace-Id ahead of every resource-derived header, including those for connection, source and destination identifiers. Endpoints whose declared request bodies carry only a resource identifier are nonetheless reached with an added workspaceId field, because the extractor reads the body rather than the endpoint's schema, so the permission check is performed against the workspace the caller nominated while the handler acts on the resource identifier the caller supplied. Nothing afterwards compares the resource's owning workspace with the one that was authorized. A member of any workspace can therefore read source and destination configuration, trigger and cancel syncs, and delete connections, sources and destinations that belong to workspaces they have no access to, at whatever privilege level their own workspace membership grants them.	2026-08-25	8.8	CVE-2026-80049
AJCloud--AJY IPC Firmware	AJCloud AJY IPC firmware prior to version 01.10715.11.37 contains a path traversal vulnerability in the jdbhttpd web service that allows unauthenticated remote attackers to read arbitrary files with root privileges by supplying path traversal sequences in the HTTP request URI. Attackers can send crafted HTTP requests to port 80 without authentication to access sensitive files including cleartext RTSP credentials, Wi-Fi SSID and pre-shared key, device serial number, and cloud binding parameters.	2026-08-30	7.5	CVE-2026-56718
alibaba-fusion--next	A security flaw has been discovered in alibaba-fusion next up to 1.27.34. This issue affects the function ConfigProvider.getContextProps of the file components/dialog/index.tsx of the component deepMerge. Performing a manipulation of the argument locale results in improperly controlled modification of object prototype attributes. The attack may be initiated remotely. The reported GitHub issue was closed automatically due to inactivity.	2026-08-24	7.3	CVE-2026-78180
Alluxio--alluxio	Alluxio's S3 REST proxy fails to verify AWS Signature Version 4 signatures in its default configuration, allowing unauthenticated attackers to spoof user identity. Attackers can extract usernames from unsigned Authorization headers and impersonate any user, including service accounts, to read, write, and delete arbitrary data.	2026-08-25	9.8	CVE-2026-79787
amazon--amazon-ssm-agent	Improper limitation of a pathname to a restricted directory in the aws:downloadContent plugin in amazon-ssm-agent before 3.3.4515.0 might allow an authenticated remote user whose ssm:SendCommand permission is restricted to the AWS-DownloadContent document, to write arbitrary files outside the intended download directory with root privileges, via crafted object keys in the S3	2026-08-28	8.8	CVE-2026-81849

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	source the document is directed to retrieve. This issue may lead to arbitrary code execution as root if specific sensitive files are overwritten. To remediate this issue, customers should upgrade amazon-ssm-agent to version 3.3.4515.0 or later.			
Amazon--strands-agents-tools	Improper neutralization of input used for LLM prompting in the python_repl tool in Amazon Strands Agents Tools before 0.8.5 might allow remote actors to execute arbitrary Python code on the agent's host by bypassing the human consent gate, via a crafted prompt that forwards non_interactive_mode as a keyword argument through the batch tool. To remediate this issue, users should upgrade to version 0.8.5 or later.	2026-08-25	8.1	CVE-2026-78379
AmpleByte Pvt Limited--Brave Conversion Engine (PRO)	Unauthenticated Cross Site Scripting (XSS) in Brave Conversion Engine (PRO) <= 0.8.6 versions.	2026-08-24	7.1	CVE-2026-32476
Andyyyy64--whichllm	whichllm before 0.5.16 contains a code injection vulnerability in the run and snippet commands that allows a remote attacker who controls a HuggingFace repository to achieve arbitrary code execution by crafting a malicious GGUF filename containing double quotes or other special characters. The script generation function in cli.py interpolates HuggingFace-derived values, including GGUF variant filenames from the Hub API siblings rfilename field, directly into Python source code without escaping, allowing the crafted filename to break out of the generated string literal and execute injected code on the user's machine before any model download occurs.	2026-08-26	8.8	CVE-2026-58474
apify--actors-mcp-server	The get-html-skeleton tool fetched a URL the caller supplied after checking only its syntax. The handler in src/tools/common/get_html_skeleton.ts validated the url argument with isValidHttpRequest from src/utlis/generic.ts, which confirmed the string began with an http or https scheme and parsed as a URL and inspected neither the host name nor the address it resolves to. Loopback, link-local and private ranges therefore passed, including the address cloud providers use to serve instance metadata. The unchecked URL was handed to the web-browser actor and the fetched document was returned in the tool response, so any caller of the MCP server could make it request an endpoint reachable only from the host and read the result, including instance credentials. Version 0.9.12 removes the tool.	2026-08-27	8.6	CVE-2026-81093
apitable--apitable	APITable through 1.13.0-beta.1 annotates both getUserHistories and closePausedUserAccount in InternalUserController with requiredLogin = false. ResourceInterceptor honours that annotation by returning before any session or API key is validated, and the nginx gateway shipped with the product proxies every /api request to the backend server, so both endpoints are reachable by any unauthenticated client that can reach the gateway. An attacker can POST to /api/v1/internal/getUserHistories to enumerate the accounts sitting in the 30-day cooling-off period that follows a deletion request, then POST to /api/v1/internal/users/{userId}/close for each one. The closure path clears the account's email address, phone number and nickname, cancels its space subscriptions, removes its space memberships and deletes its OAuth bindings, so the cooling-off window that exists to let a user reverse a deletion request is bypassed and the account cannot be recovered.	2026-08-27	8.2	CVE-2026-80208
Applied Systems Engineering--ASE2000 V2	ASE2000 2.35 through 2.37 is vulnerable to an improper certificate validation vulnerability, which may allow an attacker to impersonate the trusted peer, complete the TLS handshake, and read or modify protected communications.	2026-08-27	7.4	CVE-2026-18717
argoproj--argo-rollouts	Argo Rollouts dashboard through 1.10.0 binds to all interfaces and exposes mutating Rollout operations without authentication, authorization, or CSRF protection. Attackers on the same network can invoke PromoteRollout, AbortRollout, RestartRollout, SetRolloutImage, UndoRollout, and RetryRollout operations across all namespaces accessible to the operator's kubeconfig.	2026-08-28	9.8	CVE-2026-82277
argoproj-labs--argocd-mcp	argocd-mcp 0.8.0 binds its HTTP transport to every network interface and accepts MCP sessions without requiring caller credentials when ARGOCD_API_TOKEN is configured. Attackers who can reach the listener can invoke the full tool surface using the operator's stored token to create applications, request syncs, and modify Argo CD resources.	2026-08-29	10	CVE-2026-82456
Autodesk--3ds Max	A maliciously crafted ABC file, when parsed through Autodesk 3ds Max, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	2026-08-24	7.8	CVE-2026-16783

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Autodesk--3ds Max	A maliciously crafted SVG file, when parsed through Autodesk 3ds Max, can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to execute arbitrary code in the context of the current process.	2026-08-24	7.8	CVE-2026-19568
Autodesk--3ds Max	A maliciously crafted FLT file, when parsed through Autodesk 3ds Max, can force an Out-of-Bounds Write vulnerability. A malicious actor may leverage this vulnerability to cause a crash, cause data corruption, or execute arbitrary code in the context of the current process.	2026-08-24	7.8	CVE-2026-7455
AUTOMATIC111--stable-diffusion-webui	Stable Diffusion WebUI through 1.10.1 contains a credential disclosure vulnerability in the /sdapi/v1/cmd-flags endpoint that returns parsed command-line arguments including gradio_auth and api_auth values in cleartext. Unauthenticated attackers can access this endpoint to retrieve configured usernames and passwords, then use them to authenticate to the interface and access the application.	2026-08-28	7.5	CVE-2026-82288
aws--diagram-as-code	A relative path traversal issue in the zip extraction functionality in AWS diagram-as-code (awsdac) in versions 0.10 through 0.23 can allow a third party to write arbitrary files to the local filesystem via crafted zip entry names containing path traversal sequences. This could allow the third party to perform inappropriate actions in the diagram bundle. To remediate this issue, users should upgrade to the version 0.24 or later.	2026-08-27	7.1	CVE-2026-81838
axew3--WP w3all phpBB	Unauthenticated Cross Site Scripting (XSS) in WP w3all phpBB <= 3.0.6 versions.	2026-08-27	7.1	CVE-2026-78293
AzuraCast--AzuraCast	AzuraCast exposes the Liquidsoap custom configuration fields through an endpoint that does not require the permission guarding them. The backend_config property in backend/src/Entity/Station.php is annotated with GROUP_GENERAL, and PUT /api/station/{station_id}/profile/edit in backend/src/Controller/Api/Stations/ProfileEditController.php deserializes with that group while requiring only StationPermissions::Profile. AbstractArrayEntity::fromArray() then assigns every public property with no field-level permission check, so custom_config_top, custom_config, custom_config_pre_playlists, custom_config_pre_live, custom_config_pre_fade and custom_config_bottom are writable through it. ConfigWriter::writeCustomConfigurationSection() emits those values verbatim into the generated Liquidsoap .liq script, where the process.run() and process.exec() built-ins execute operating system commands when the backend restarts, which the built-in sync task triggers automatically once needs_restart is set. The dedicated endpoint for the same data, PUT /api/station/{id}/liquidsoap-config, requires StationPermissions::Broadcasting, so a station manager holding only the profile permission reaches configuration that the intended boundary reserves for broadcasting operators.	2026-08-24	8.8	CVE-2026-76836
Baserow--Baserow	Baserow dispatches an Application Builder data source without acting on the result of its permission check. The dispatch and record-name views in backend/src/baserow/contrib/builder/api/data_sources/views.py are declared with a permission class that admits any caller, so a request carrying no credential reaches the handler. DataSourceService.dispatch_data_sources in backend/src/baserow/contrib/builder/data_sources/service.py then calls check_multiple_permissions without asking it to raise, and neither stores nor examines the mapping of denials it returns, so a denied check leaves execution to continue and the data source is dispatched whatever the caller's identity. The dispatch runs with the integration's own credentials, so an unauthenticated request naming a data source receives the rows and fields that source reads. Identifiers are small integers and can be enumerated. Version 2.3.1 passes raise_exception to the same call.	2026-08-27	7.5	CVE-2026-81335
bdthemes--SigmaForms Pro AI Generated Forms	The Sigma Forms Pro plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.4.5 via the handle_form_submission function. This is due to the plugin dynamically granting the unfiltered_upload capability to all users during form submissions and bypassing MIME type validation when allowed_file_types is not configured. This makes it possible for unauthenticated attackers to execute code on the server. Several default pre-built templates including Job Application, Support Ticket, and Wholesale Application have file upload fields with no file type restrictions configured by design, making this vulnerability immediately exploitable upon installation.	2026-08-29	9.8	CVE-2026-14494
Bendix--EC80ESP+ J1708	Bendix EC80 Brake ECU is vulnerable to a stack-based buffer overflow, which may allow an attacker to crash the ECU. A crafted payload can then be used to remotely	2026-08-27	7.5	CVE-2026-67560

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execute arbitrary code or inject arbitrary CAN bus traffic. This could cause the loss of the ABS function, steering assist, speedometer, and shifting.			
better-auth--sso	@better-auth/sso before 1.6.27 (and before 1.4.8 in the 1.4.x line and before 1.7.0-rc.5 in the 1.7 prerelease line) contains two domain-ownership flaws. When domain verification is disabled, automatic organization assignment accepts unverified provider domains, allowing an authenticated organization owner/administrator to register an SSO provider for an arbitrary domain and have users with matching email domains added to the attacker's organization with default member permissions. When domain verification is enabled, a race condition between the verify-domain and update-provider endpoints can apply completed DNS proof to a different domain; combined with implicit account linking, this can link an attacker-controlled identity provider to an existing user account. Exploitation requires the SSO plugin (and, for the org-assignment path, the organization plugin) with the relevant configuration enabled.	2026-08-25	8.1	CVE-2026-80192
bookstackapp--bookstack	BookStack before 26.05.4 contains a remote code execution vulnerability in the portable ZIP import functionality that allows users with Import Content and Create Books permissions to upload a PHP polyglot file as a book cover. Attackers can bypass image extension validation by embedding a PHP file with a .php filename in the ZIP archive, which is stored in the public web root and executed by unauthenticated requests.	2026-08-29	8.8	CVE-2026-82450
boxpositron--with-context-mcp	A flaw has been found in boxpositron with-context-mcp up to 3.0.7. This affects the function ingest_notes/teleport_notes/sync_notes/project_folder of the file src/index.ts. Executing a manipulation can lead to path traversal. It is possible to launch the attack remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-27	7.3	CVE-2026-81491
Brainstorm Force--SureFeedback Client Site	Subscriber Sensitive Data Exposure in SureFeedback Client Site <= 1.2.12 versions.	2026-08-27	7.5	CVE-2026-80433
budibase--server	Budibase versions before 3.41.3 contain a remote code execution vulnerability in plugin handling that allows authenticated admin users to execute arbitrary code by uploading a malicious plugin tarball. The server calls eval() on plugin JavaScript files without sandboxing in the main Node.js process, enabling attackers to exfiltrate environment variables and credentials with root privileges in default deployments.	2026-08-28	9.1	CVE-2026-82244
budibase--server	Budibase before 3.41.3 fails to enforce per-table role restrictions on the POST /api/datasources/query endpoint, allowing low-privilege BASIC users to read, create, update, or delete rows in any table regardless of configured permissions. Attackers with BASIC role can submit crafted query requests with target table identifiers to bypass table-level access controls and manipulate restricted data.	2026-08-28	8.1	CVE-2026-82239
budibase--server	Budibase before 3.41.3 fails to validate app-scoped builder role assignments in the public user create and update endpoints, allowing an authenticated app-scoped builder to grant builder access to unrelated apps. Attackers can submit crafted requests to the user update API with builder.apps fields to escalate privileges and gain unauthorized builder access to other applications in the same tenant.	2026-08-28	8.1	CVE-2026-82240
budibase--server	Budibase before 3.41.3 fails to enforce role-based authorization on license management endpoints, allowing any authenticated user to delete license keys or manipulate offline tokens. Attackers with basic user privileges can access /api/global/license/* endpoints to disable premium features and downgrade deployments for all users.	2026-08-28	8.1	CVE-2026-82245
budibase--server	Budibase backend-core (@budibase/backend-core, as used by @budibase/server) omits the shared address space range 100.64.0.0/10 from its default SSRF blacklist (DEFAULT_BLACKLIST) used by REST datasource query previews. When the default blacklist is active (i.e., a self-hosted deployment has not defined BLACKLIST_IPS), an authenticated user with the Builder permission can submit a REST datasource query preview request to POST /api/queries/preview targeting a reachable HTTP(S) service in the 100.64.0.0/10 range, causing the server to send a request to that target and return its response through the preview flow. Per the advisory, no released fix was identified at the time of publication; remediation is to add 100.64.0.0/10 to DEFAULT_BLACKLIST.	2026-08-28	7.1	CVE-2026-82241
budibase--server	Budibase versions before 3.41.3 contain a missing authorization vulnerability in the POST /api/resources/duplicate endpoint that allows authenticated builders to inject tables, automations, queries, and screens into any other application without holding any role in the destination workspace. Attackers can inject resources by specifying an arbitrary destination workspace ID in the request body, then trigger	2026-08-28	7.7	CVE-2026-82242

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injected automations with outgoing webhooks to exfiltrate data from victim applications.			
budibase--server	Budibase Server before 3.41.3 contains a server-side request forgery vulnerability in the datasource verify endpoint that allows builder-level users to supply arbitrary URLs without SSRF validation. Attackers can exploit this to leak internal CouchDB credentials by making requests to attacker-controlled servers, gaining full database access in cloud deployments.	2026-08-28	7.6	CVE-2026-82243
budibase--server	Budibase Server before 3.41.3 contains a server-side request forgery vulnerability in the query import endpoint that fails to validate user-supplied URLs before fetching content. Attackers can submit arbitrary URLs to retrieve responses from internal services including cloud metadata endpoints and other restricted network resources.	2026-08-28	7.1	CVE-2026-82246
BuilderIO--gpt-crawler	gpt-crawler through 1.5.1 fails to validate the outputFileName parameter in the POST /crawl endpoint, allowing unauthenticated attackers to write arbitrary files to any filesystem path. Attackers can supply absolute paths or parent-directory segments to overwrite existing files with content sourced from attacker-controlled URLs.	2026-08-28	8.6	CVE-2026-82286
bytedance--UI-TARS-desktop	startServer.ts in the mcp-http-server package of UI-TARS-desktop defaulted its listen address to ':::' when no host was given, so startSseAndStreamableHttpMcpServer bound the Streamable HTTP and SSE MCP transports to every interface, and its authentication middleware was optional: middlewares are applied only when a caller supplies them. The @agent-infra/mcp-server-commands and @agent-infra/mcp-server-filesystem entry points call startSseAndStreamableHttpMcpServer with a host and port alone and pass no middleware, so neither server required a credential. The commands server exposes a run_command tool that hands its caller-supplied command string to promisify(child_process.exec), so any unauthenticated client able to reach the port could run arbitrary commands as the user running the server, and the filesystem server exposed its file read and write tools on the same terms. The listen default became 127.0.0.1 in commit c2ad42e3eb9b27830db41a3e6f51ca7179d9b168; the package version stayed at 1.2.4 across that change, so the boundary is the commit rather than a release.	2026-08-27	10	CVE-2026-81735
CalcProgrammer1--OpenRGB	Arbitrary file overwrite via SAVE_PROFILE message in OpenRGB. This issue affects OpenRGB through 1.0rc3.	2026-08-26	9.1	CVE-2026-59682
CalcProgrammer1--OpenRGB	The OpenRGB network protocol allows to write attacker controlled strings into arbitrary file system paths (extension of CVE-2026-59682). This allows either a full system compromise from local or remote (if the daemon is running as root) or a full account takeover (if the daemon is running in user context).	2026-08-26	9.8	CVE-2026-59683
CalcProgrammer1--OpenRGB	The OpenRGB network protocol allows attackers to cause memory exhaustion and out-of-bounds memory reads and writes by passing inconsistent data.	2026-08-26	8.2	CVE-2026-18794
Canonical--LXD	A path traversal vulnerability in LXD's instance template processing allows an attacker with container edit permissions, or any user launching a crafted image, to overwrite arbitrary files on the host system as root. When processing target template paths specified in metadata.yaml, LXD validates the path against a confined os.Root directory handle but subsequently opens and creates the file using os.Create with an unconfined string path. This discrepancy between path resolution checks and file creation allows an attacker to escape directory confinement, overwrite root-owned host files, and achieve host root code execution.	2026-08-24	9.9	CVE-2026-66897
CAYIN Technology--CAYIN CMS-WS	CAYIN CMS-WS, CMS-SE, and SMP series products developed by CAYIN Technology have an Arbitrary File Upload vulnerability. Privileged remote attackers can upload and execute web shells backdoors, thereby enabling arbitrary code execution on the server.	2026-08-26	7.2	CVE-2026-80233
cbcoutinho--nextcloud-mcp-server	Nextcloud MCP Server is a production-ready MCP server that connects AI assistants to a Nextcloud instance. Prior to 0.117.2, the POST /webhooks/nextcloud endpoint in nextcloud_mcp_server/vector/webhook_receiver.py has no authentication by default because WEBHOOK_SECRET defaults to None and startup validation does not require it. When WEBHOOK_SECRET is unset, handle_nextcloud_webhook() accepts unauthenticated requests. The payload["user"]["uid"] field parsed in nextcloud_mcp_server/vector/webhook_parser.py is attacker-controlled and is used without an authenticated-session cross-check for Qdrant operations, allowing a network attacker to delete or trigger re-indexing of vector embeddings for any user and to destroy the semantic search index by sending forged deletion events. This issue is fixed in version 0.117.2.	2026-08-25	9.1	CVE-2026-55640

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ceph--ceph	Ceph is an open-source distributed storage platform providing object, block, and file storage. In versions prior to 20.2.4 and 19.2.6, the Monitor subscription handler fails to properly authorize access to the configuration-key store, allowing any CephX user with only `mon allow r` capabilities to read the entire store by sending a single crafted MMonSubscribe message. The config-key store holds sensitive secrets including OSD LUKS disk-encryption passphrases and, on cephadm-managed clusters, the SSH private key that cephadm uses to reach every host in the cluster. Because that key grants root on every node under the default cephadm configuration, a low-privileged read-only account can escalate to full cluster and host compromise. This issue is fixed in versions 20.2.4 and 19.2.6	2026-08-27	9.1	CVE-2026-50152
ceph--ceph	Ceph is an open-source distributed storage platform providing object, block, and file storage. In versions prior to 20.2.4 and 19.2.6, the CephX authentication protocol encrypts tickets with AES-128-CBC in an unauthenticated mode that uses a hard-coded initialization vector and no message authentication, allowing an attacker to forge credentials and gain cluster-wide access. Because the ciphertext is malleable and the monitor will encrypt attacker-chosen entity names, an attacker holding one low-privilege key and able to observe CephX traffic can use the monitor as an encryption oracle and splice ciphertext blocks into valid tickets for privileged entities such as Manager, MDS, and OSD. The same lack of authentication also lets an attacker with CephX permissions escalate privileges by flipping a single bit in a service ticket to set its allow_all field to true. This issue is fixed in versions 20.2.4 and 19.2.6.	2026-08-27	8.9	CVE-2025-30156
ceph--ceph	Ceph is an open-source distributed storage platform providing object, block, and file storage. In versions prior to 20.2.4 and 19.2.6, the RADOS Gateway (RGW) protects STS session tokens with an AES-128-CBC handler that provides no message authentication, allowing an attacker who holds any valid STS token to tamper with it undetected and escalate to full RGW administrative access. Because the ciphertext is unauthenticated, the attacker can perform a CBC bit-flip on the acct_type, perm_type, and is_admin fields of their own token, and a forged is_admin value triggers a global administrative override that bypasses all capability checks. The attack is reachable remotely over the RGW S3 endpoint and is a self-contained modification of a token the attacker already possesses, requiring no encryption oracle and no network observation. It requires only a single valid STS token, which need not carry any elevated privileges, with STS enabled. This issue is fixed in versions 20.2.4 and 19.2.6.	2026-08-27	8.8	CVE-2026-39944
ceph--ceph	Ceph is an open-source distributed storage platform providing object, block, and file storage. In versions prior to 20.2.4 and 19.2.6, the Ceph Object Gateway (RGW) SigV4 handler does not reject requests that carry x-amz-* headers absent from the signed header set, allowing anyone holding a presigned URL to attach arbitrary unsigned x-amz-* headers that RGW will honor. AWS S3 requires every x-amz-* header on a SigV4 request to be signed and rejects requests bearing additional unsigned headers, but RGW validates only the headers listed in X-Amz-SignedHeaders and ignores any extra ones, so they take effect without being covered by the signature. By adding such headers to a presigned PUT URL, an attacker can grant themselves more capabilities than the URL's signer intended and escalate their privileges. This issue is fixed in versions 20.2.4 and 19.2.6.	2026-08-27	8.1	CVE-2026-54330
Chainlit--chainlit	Chainlit is a Python framework for building production-ready conversational AI applications. From 2.4.0rc0 until 2.12.0, Chainlit deployments with features.mcp.enabled set to true in .chainlit/config.toml expose the POST /mcp endpoint without requiring authentication. For stdio transport, the endpoint accepts a user-controlled fullCommand string. The validate_mcp_command() function in backend/chainlit/mcp.py checks only the executable name against config.features.mcp.stdio.allowed_executables and passes unchecked arguments to StdioServerParameters in backend/chainlit/server.py. Because npx supports the -c argument, an attacker can execute arbitrary shell commands with the privileges of the Chainlit process. If allowed_executables is unset, its None default is treated as allowing every executable. This issue is fixed in version 2.12.0.	2026-08-25	9.8	CVE-2026-45018
Chainlit--chainlit	Chainlit is a Python framework for building production-ready conversational AI applications. From 2.4.0rc0 until 2.12.0, Chainlit deployments with features.mcp.enabled set to true in .chainlit/config.toml expose the POST /mcp endpoint without requiring authentication. For sse and streamable-http transports, ConnectSseMCPRequest and ConnectStreamableHttpMCPRequest in backend/chainlit/types.py accept a user-controlled url and optional headers dictionary without scheme validation, private-address filtering, or an allowlist. The connect_mcp handler in backend/chainlit/server.py passes these values to	2026-08-25	7.2	CVE-2026-45019

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sse_client() or streamablehttp_client(), allowing the Chainlit server to make blind outbound requests to arbitrary internal or external services, including cloud metadata endpoints, with attacker-controlled Authorization and Cookie headers. The SSE URL sink has existed since 2.4.0rc0, while attacker-controlled header forwarding and streamable-http support were added in 2.6.4. The response is consumed internally and not returned, but the attacker can issue state-changing authenticated requests, discover internal services, scan ports, and probe metadata endpoints. This issue is fixed in version 2.12.0.			
ChatGPTNextWeb--NextChat	NextChat versions from 2.15.8 through 2.16.1 contain an improper URL validation vulnerability in the proxy endpoint that allows attackers to obtain the server's OpenAI API key. The x-base-url header is validated using substring matching instead of hostname parsing, allowing any URL containing 'api.openai.com' to pass validation and receive the server's credentials in the Authorization header.	2026-08-30	7.5	CVE-2026-82639
Cinnamon--kotaemon	Kotaemon through 0.12.0 fails to properly validate conversation ownership in select_conv, delete_conv, rename_conv, and on_set_public_conversation functions in control.py. Attackers can read other users' chat histories, delete conversations, or rename conversations by supplying arbitrary conversation identifiers without proper authorization checks.	2026-08-28	7.4	CVE-2026-82281
cleverbrush--framework	A vulnerability has been found in cleverbrush framework and deep up to 4.4.0. This impacts the function deepExtend of the file libs/deep/src/deepExtend.ts. The manipulation leads to improperly controlled modification of object prototype attributes. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. Upgrading to version 4.4.1 will fix this issue. The identifier of the patch is 810398c1308c500c3b8b6af380b5a89371389327. You should upgrade the affected component.	2026-08-25	7.3	CVE-2026-78654
Cloud Foundry--bosh-vsphere-cpi-release	Traffic interception vulnerability in BOSH Director vCenter CPI allows attackers positioned between BOSH Director and vCenter to impersonate vCenter REST API and capture administrator credentials via HTTP Basic auth, leading to complete virtualization infrastructure takeover. An attacker who can intercept traffic between the BOSH Director and vCenter can establish a malicious server impersonating the vCenter REST API. When the BOSH Director makes CPI calls to perform routine cloud infrastructure operations, the attacker captures the vCenter administrator username and password transmitted via HTTP Basic authentication. The vulnerability stems from insufficient authentication security in the communication protocol between BOSH Director and vCenter. While HTTPS may be used, the lack of proper certificate validation and pinning allows attackers to successfully impersonate vCenter endpoints. Because vCenter credentials typically grant full administrative control over the entire virtualization estate, successful credential capture yields complete takeover of every VM, datastore, and network the CPI manages. This exposure exists on every CPI call (including routine deployment operations, not just when tags are configured) and cannot be mitigated by supplying a CA certificate alone. The attack impacts all infrastructure managed by the compromised vCenter instance, potentially affecting hundreds or thousands of VMs across multiple deployments and environments.	2026-08-29	7.7	CVE-2026-41012
Cloud Foundry--UAA	Improper handling of case sensitivity (CWE-178) in the identity zone authorization check in the Identity Zone Endpoint in Cloud Foundry UAA allows a remote authenticated attacker holding only the zones.write authority to bypass the intended restriction that this authority does not grant access to the privileged uaa (system) identity zone, by referring to the zone identifier in a non-lowercase form (e.g. UAA) in the request path and body. The authorization layer performs a case-sensitive comparison against the system zone identifier, while the underlying MySQL persistence layer resolves identifiers case-insensitively under its default collation, so the request is authorized incorrectly and is then resolved against the real system zone record. This allows the attacker to overwrite the system zone's JWT signing key with attacker-controlled key material, forge JWTs claiming the admin client and administrator scopes, and fully compromise UAA and any Cloud Foundry deployment that trusts it. This issue only affects UAA deployments backed by MySQL using its default collation; PostgreSQL and HSQLDB backends are not affected.	2026-08-25	8.7	CVE-2026-59335
Code for Recovery--12 Step Meeting List	Unauthenticated Cross Site Scripting (XSS) in 12 Step Meeting List <= 3.19.16 versions.	2026-08-24	7.1	CVE-2026-66584

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Simple Inventory System	A vulnerability was identified in code-projects Simple Inventory System 1.0. This vulnerability affects unknown code of the file /InventoryManagement/edit.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2026-08-25	7.3	CVE-2026-79845
codepeople--CP Media Player	Unauthenticated Cross Site Scripting (XSS) in CP Media Player <= 1.3.0 versions.	2026-08-27	7.1	CVE-2026-78281
codepeople--Music Player for WooCommerce	Unauthenticated Cross Site Scripting (XSS) in Music Player for WooCommerce <= 1.8.9 versions.	2026-08-27	7.1	CVE-2026-78283
CODEPRESS IT Solutions LLC--Visitor Traffic Real Time Statistics Pro	Unauthenticated SQL Injection in Visitor Traffic Real Time Statistics Pro <= 11.17 versions.	2026-08-27	9.3	CVE-2026-32479
coderaiser--cloudcmd	Cloud Commander before 19.20.2 contains a directory traversal vulnerability in REST file-operation and markdown endpoints that fails to properly validate path normalization. Attackers can use path traversal sequences to read, write, move, or copy files outside the configured root directory.	2026-08-29	9.8	CVE-2026-82460
coderamp-labs--gitingest	Gitingest through 0.3.1 fails to properly validate hostnames in _validate_host, accepting any host with a git., gitlab., or github. prefix regardless of known-hosts list membership. Attackers can submit URLs with attacker-controlled hostnames to trigger outbound connections to arbitrary hosts and disclose GitHub personal access tokens via HTTP basic credentials.	2026-08-28	7.4	CVE-2026-82289
collective--icalendar	icalendar is an RFC 5545 compatible parser and generator of iCalendar files for Python. From 7.1.0 until 7.1.3, the Component equality method in src/icalendar/cal/component.py compares nested subcomponents with two membership loops, and each membership test invokes the same method on child components, causing O(2^n) work relative to nesting depth. Component.from_ical accepts arbitrarily nested BEGIN:VEVENT blocks without a depth limit, so an attacker can submit a sub-kilobyte .ics file containing equal nested subtrees and trigger the cost when an application performs equality, inequality, membership, deduplication, test-assertion, round-trip, or normalization comparisons. Parsing alone does not trigger the issue, and comparisons that differ early short-circuit, but a few hundred bytes can pin a CPU core for minutes or indefinitely, causing denial of service in calendar sync or import endpoints, invite processing, and other comparison paths. This issue is fixed in version 7.1.3.	2026-08-25	7.5	CVE-2026-55099
Combodo--iTop	Combodo iTop is a web-based IT service management tool. Prior to 3.2.3, iTop is vulnerable to Reflected Cross-Site Scripting (XSS) in the dashboard revert functionality. This issue has been fixed in version 3.2.3.	2026-08-24	8.9	CVE-2026-30864
Combodo--iTop	Combodo iTop is a web-based IT service management tool. Prior to 3.2.3, iTop is vulnerable to PHP object injection in the user preference functionality, which can lead to remote code execution. This issue has been fixed in version 3.2.3.	2026-08-24	8.7	CVE-2026-40877
continuedev--continue	The Continue CLI applies an incomplete denylist as its only barrier to destructive shell commands when running unattended. In headless mode and auto mode the default policy in extensions/cli/src/permissions/defaultPolicies.ts grants the Bash tool the allow permission, and permissionChecker.ts hard-blocks a command only when the terminal-security evaluator returns a disabled verdict, so isCriticalCommand in packages/terminal-security/src/evaluateTerminalCommandSecurity.ts is the sole control. Its dangerous-path test matches only /, /*, ~, ~/*, /usr, /etc, /bin and /sbin and their prefixes, so a recursive forced removal of /home, /root, /var, /opt or /srv is not disabled. The command line is parsed with shell-quote, which reduces \$HOME to an empty token, so rm -rf \$HOME also fails the dangerous-path test while the shell re-expands the variable when the command is spawned. find with -delete is rated high risk rather than disabled, and shred, wipafs, truncate and pkexec are not handled. Because the agent autonomously reads content it does not control, including fetched web pages, repository files and issue text, an indirect prompt injection in that content can cause an unattended run to destroy the invoking user's data.	2026-08-24	7.4	CVE-2026-76072
coroot--coroot	Coroot's unauthenticated MCP OAuth dynamic client registration endpoint accepts any syntactically valid redirect URI without validation, allowing attackers to register clients pointing to attacker-controlled hosts. Attackers can send authorization URLs to signed-in users, capture their authorization codes upon consent approval, and exchange them for access tokens to hijack MCP sessions.	2026-08-25	7.1	CVE-2026-79786

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cozmoslabs--TranslatePress	Unauthenticated Privilege Escalation in TranslatePress <= 3.3.2 versions.	2026-08-24	9.8	CVE-2026-78267
cozmoslabs--TranslatePress Translate Multilingual sites with AI Translation	The TranslatePress - Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.1 via the 'trp_get_translations_regular' AJAX action. This makes it possible for unauthenticated attackers to extract the raw administrator password-reset URL - including the plaintext reset key and login parameters stored in the translation dictionary table - enabling full administrator account takeover. This vulnerability is only exploitable when automatic string saving is enabled (the default setting) and the target administrator's profile locale is set to a published secondary language, as these conditions cause the password-reset URL to be persisted as a translatable string in the secondary-language dictionary table.	2026-08-26	9.8	CVE-2026-19632
cozmoslabs--TranslatePress Translate Multilingual sites with AI Translation	The TranslatePress - Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Noise-Key Injection into HTML Parser in all versions up to, and including, 3.3.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation is possible because WordPress's comment KSES allowlist permits the payload structure - an anchor tag with href and title attributes alongside a code tag - causing the malicious comment to be stored verbatim in the database, where it is later processed by the vulnerable parser during page translation.	2026-08-28	7.2	CVE-2026-76053
crater-invoice-inc--crater	Crater Invoice through 6.0.6 contains a path traversal vulnerability in the self-update API that allows authenticated company owners to write arbitrary files outside the intended extraction directory by supplying crafted ZIP archives with ../sequences to the unzip endpoint. Attackers can exploit unsanitized ZIP entry names passed to PHP's ZipArchive::extractTo() to write arbitrary PHP files into the web-accessible public directory and achieve remote code execution on the server.	2026-08-25	8.8	CVE-2026-57863
creativemindssolutions--CM Map Locations Visualize and share your locations in a few clicks	The CM Map Locations - Visualize and share your locations in a few clicks plugin for WordPress is vulnerable to Limited Arbitrary File Upload in all versions up to, and including, 2.1.8 via the uploadMedia function. This is due to insufficient file type validation in the upload handler, which performs incomplete extension filtering without MIME-type checks or upload capability verification before passing attacker-supplied files to move_uploaded_file(). This makes it possible for authenticated attackers, with subscriber-level access and above, to upload files that may be executable, which makes remote code execution possible. The required nonce is exposed to any logged-in Subscriber via the CMLOC_Editor_Images JavaScript object on the front-end location editor page.	2026-08-25	8.8	CVE-2026-16601
Crocoblock--JetEngine	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetEngine allows Reflected XSS. This issue affects JetEngine: from n/a through 3.8.14.2.	2026-08-28	7.1	CVE-2026-81760
cyberlord92--SAML Single Sign On SSO Login	The SAML Single Sign On - SSO Login plugin for WordPress is vulnerable to Authentication Bypass in versions up to, and including, 5.4.6. This is due to the mo_saml_login_validate() ACS handler persisting the X.509 certificate extracted from an incoming SAMLResponse into the mo_saml_required_certificate option before the signature-validation verdict is enforced, because mo_saml_find_certificate() returns false on a fingerprint mismatch rather than halting execution. This makes it possible for unauthenticated attackers to overwrite the plugin's stored IdP signing certificate with an attacker-controlled value, and subsequently forge SAML assertions for any WordPress account - including administrators - to obtain a fully privileged session. Note: The exploit requires the administrator to perform a repair after receiving the test_config_error_wpsamlerr004 error message during the test configuration.	2026-08-29	7.5	CVE-2026-75807
D-Link--DIR-825M	A vulnerability was detected in D-Link DIR-825M 1.1.8. This affects the function sub_46725C of the file /boafm/formDiskFormat of the component Disk Formatting Handler Endpoint. The manipulation of the argument partition results in stack-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used.	2026-08-30	9.9	CVE-2026-82592
D-Link--DIR-825M	A flaw has been found in D-Link DIR-825M 1.1.8. This impacts the function sub_41802C of the file /boafm/formLtefotaUpgradeFibocom of the component LTE Module Firmware Upgrade. This manipulation of the argument fota_url causes stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been published and may be used.	2026-08-30	9.9	CVE-2026-82593

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
D-Link--DIR-825M	A vulnerability was found in D-Link DIR-825M 1.1.8. Affected by this vulnerability is the function sub_456CF4 of the file /boafrm/formSysCmd of the component System Command Execution. Performing a manipulation of the argument sysCmd results in command injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	2026-08-30	7.4	CVE-2026-82595
dahlia--logtape	LogTape is an unobtrusive logging library. Prior to 1.3.11, 2.0.14, and 2.1.5, the @logtape/syslog package's escapeStructuredDataValue() function in packages/syslog/src/syslog.ts does not neutralize C0 control characters from U+0000 through U+001F in structured data values, and formatStructuredData() inserts property keys without validating the RFC 5424 SD-NAME grammar. When includeStructuredData is true, an attacker-controlled newline can terminate an RFC 6587 non-transparent TCP syslog frame and make following bytes appear as a forged RFC 5424 record, while a key containing a closing bracket or other forbidden character can terminate or corrupt the structured-data element. Applications that forward attacker-controlled property values or keys can therefore allow forged records with arbitrary hosts, applications, process identifiers, facilities, or severity levels, undermining downstream collector and SIEM integrity. This issue is fixed in versions 1.3.11, 2.0.14, and 2.1.5.	2026-08-26	8.6	CVE-2026-54511
Dassault Systmes--3DSwymer	An Improper Authorization vulnerability affecting 3DPassport in 3DSwymer from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2026x could allow an attacker to gain access to some user accounts.	2026-08-27	9.3	CVE-2026-16279
Dassault Systmes--Tuleap Enterprise Edition	A Use of Default Password vulnerability affecting Tuleap Enterprise Edition from 17.0 through 17.5 could allow an attacker to gain access to user accounts created during XML import.	2026-08-25	7.7	CVE-2026-19851
DataDog--dd-trace-rs	dd-trace-rs provides Datadog application performance monitoring for Rust. From 0.1.0 until 0.3.3, datadog-opentelemetry/src/propagation/tracecontext.rs parses the W3C tracestate header and collects every semicolon-separated key and value pair in the Datadog dd=... vendor entry into a HashMap without enforcing a pair count or entry size limit. Because tracecontext extraction is enabled by default, a remote unauthenticated attacker can send an arbitrarily large dd=... entry and force excessive CPU and memory consumption for each request, causing denial of service in an instrumented network service. This vulnerability is fixed in 0.3.3.	2026-08-28	7.5	CVE-2026-54788
dataelement--bisheng	BISHENG before 2.6.0 contains a remote code execution vulnerability in the workflow run_once endpoint that allows authenticated users to execute arbitrary Python code. Attackers can submit crafted Code node definitions to the POST /api/v1/workflow/run_once endpoint, which executes them with exec() without sandboxing, gaining access to filesystem, credentials, and internal network resources.	2026-08-28	8.8	CVE-2026-82278
dataelement--bisheng	bisheng through 2.6.0-fix2 contains a server-side request forgery vulnerability in the POST /api/v1/workflow/report/callback endpoint that lacks authentication and applies no URL scheme restrictions or host filtering. Unauthenticated attackers can supply arbitrary URLs to enumerate internal network services and cloud metadata endpoints, then retrieve captured responses from object storage using caller-supplied object names.	2026-08-28	8.2	CVE-2026-82285
ddfourtwo--sentry-selfhosted-mcp	A security flaw has been discovered in ddfourtwo sentry-selfhosted-mcp 0.4.0. The affected element is an unknown function of the component raw_sentry_api. The manipulation of the argument endpoint results in server-side request forgery. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-26	7.3	CVE-2026-81421
dekdee--adobe-xd-mcp	A weakness has been identified in dekdee adobe-xd-mcp 1.0.0. Impacted is an unknown function of the file src/parsers/xs-parser.ts of the component file-access-from-request Endpoint. Executing a manipulation of the argument outputFile/outputDir can lead to path traversal. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-25	7.3	CVE-2026-79622
Dell--Cloud Disaster Recovery	Dell Cloud Disaster Recovery, versions 20.2 and prior, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	2026-08-26	9.1	CVE-2026-70419
Dell--Cloud Disaster Recovery	Dell Cloud Disaster Recovery, versions 20.2 and prior, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command	2026-08-26	7.2	CVE-2026-71171

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Injection') vulnerability in the REST API. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote execution.			
Dell--Power Protect Cyber Recovery	Dell PowerProtect Cyber Recovery, versions prior to 20.3, contain an Improper Authentication vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-08-26	7.6	CVE-2026-79938
Dell--PowerProtect One	Dell PowerProtect One, versions 20.1.0.0 and below, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote execution.	2026-08-26	8.8	CVE-2026-68861
Dell--PowerProtect One	Dell PowerProtect One, versions 20.1.0.0 and below, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Code execution.	2026-08-26	8.8	CVE-2026-74770
Dell--PowerProtect One	Dell PowerProtect One, versions 20.1.0.0 and below, contain a Stack-based Buffer Overflow vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Denial of service.	2026-08-26	7.5	CVE-2026-68863
Dell--ThinOS 10	Dell ThinOS 10, versions prior to 2605_10.2518, contain an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-08-24	7.8	CVE-2026-61419
deltaww--DIAEnergie	SQL Injection in Delta DIAEnergie v1.11.00.002 allows attacker to remote code execution.	2026-08-24	8.8	CVE-2026-78314
deltaww--DIAEnergie	SQL Injection in Delta DIAEnergie v1.11.00.002 allows attacker to remote code execution.	2026-08-24	8.8	CVE-2026-78315
deltaww--DIAEnergie	SQL Injection in Delta DIAEnergie v1.11.00.002 allows attacker to remote code execution.	2026-08-24	8.8	CVE-2026-78316
deltaww--DIAEnergie	SQL Injection in Delta DIAEnergie v1.11.00.002 allows attacker to remote code execution.	2026-08-24	8.8	CVE-2026-78317
DiviNext--Woo Essential	Unauthenticated SQL Injection in Woo Essential <= 4.3.0 versions.	2026-08-24	9.3	CVE-2026-32551
djust-org--djust	djust provides Phoenix LiveView-style reactive server-side rendering for Django with Rust-powered performance. Prior to 1.0.4, LiveViewConsumer.handle_mount sends a `{"type":"navigate","to":...}` frame when login_required, permission_required, or a redirecting on_mount hook denies a LiveView mount, but returns without closing the WebSocket or clearing self.view_instance. A browser follows the redirect, but a raw WebSocket client can ignore it and retain the mounted socket. Because LiveViewConsumer.handle_event does not recheck authentication or authorization, the client can send `{"type":"event",...}` frames that invoke @event_handler methods without an authenticated session, including through handle_live_redirect_mount, enabling unauthorized sensitive reads or mutations. This issue is fixed in version 1.0.4.	2026-08-25	8.2	CVE-2026-55571
documenso--documenso	Documenso before 2.13.0 accepts PDF file uploads on the /api/files/upload-pdf endpoint without requiring authentication, session tokens, or API credentials. Unauthenticated attackers can upload arbitrary PDF files indefinitely to exhaust storage resources or fill the database with unlinked document records.	2026-08-29	7.5	CVE-2026-82472
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains an improper authorization vulnerability in the Members REST API that allows attackers with only member-creation rights to reset the password of any user account, including the system administrator, without verifying password-change permissions. Attackers can supply an arbitrary user account identifier and new password in the request body to overwrite credentials and immediately lock out the legitimate account holder.	2026-08-24	8.1	CVE-2026-71504
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains an improper authorization vulnerability in the payments REST API delete endpoint that allows authenticated attackers with invoice-deletion rights to permanently delete any payment record by bypassing the intended payment-issuance rights check. Attackers can exploit this misconfigured permission check to zero paid amounts on invoices and remove entries from accounting exports, causing financial data integrity loss.	2026-08-24	8.1	CVE-2026-71506
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains a SQL injection in its CSV and XLSX import wizard. The wizard reads its update keys with GETPOST('updatekeys', 'array') in htdocs/imports/import.php, which applies only the generic alphanhtml filter: that strips HTML but leaves SQL keywords, comment markers, parentheses, spaces and quotes intact. import_insert() in htdocs/core/modules/import/import_csv.modules.php then iterates the submitted values and builds a filter with \$where[] = \$key.' = '\$data[\$key], having first applied preg_replace('/^\./i', '', \$key), an alias strip that does nothing to a value	2026-08-27	8.1	CVE-2026-81728

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	containing no dot. The assembled string is executed through \$this->db->query(). The injected SELECT resolves the row id that the import then assigns to \$lastinsertid, which becomes the WHERE target of a subsequent UPDATE, so a UNION SELECT returning an attacker-chosen integer both exfiltrates arbitrary table content and redirects which row the import overwrites; for category link tables the raw filter array is spliced into that UPDATE directly. The interface offers a fixed list of legitimate column codes but the server never checks the submitted values against it. A user holding the import permission can exploit this. Release 23.0.4 does not carry the fix; the allow-list test was added in 24.0.0.			
Dolibarr--dolibarr	Dolibarr 9.0.0 through 23.0.4 saves inbound email attachments under the name supplied in the message's MIME headers without reducing it to a safe basename. The global saveAttachment() in htdocs/emailcollector/lib/emailcollector.lib.php builds \$filepath = \$path . \$filename . '.' . \$ext and hands it to file_put_contents(), and the private saveAttachment() in htdocs/emailcollector/class/emailcollector.class.php writes to \$destdir.'/' . \$filename; the name reaches both from the attachment's own getName() or getFilename() value by way of the record-join, create-ticket and create-project operations. A traversal sequence in the filename therefore survives intact, so any sender who can email a mailbox that an EmailCollector monitors, which is the module's ordinary use for a support or ticket inbox, can place attacker-controlled content outside the per-object attachment directory without holding a Dolibarr account. Under the hardened layout Dolibarr's SECURITY.md requires, with htdocs read-only, the write is confined to the documents tree and corrupts or forges other objects' documents; where htdocs is writable the same primitive reaches a web-executable path. Version 24.0.0 applies dol_sanitizePathName() and dol_sanitizeFileName() before the write.	2026-08-27	8.2	CVE-2026-81730
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains a broken object-level authorization vulnerability in the REST API third-party site account write routes that allows authenticated attackers with third-party creation rights to overwrite the WebPortal password of any company by bypassing per-object access checks that are only enforced on read routes. Attackers can replace the victim company's WebPortal password through the write endpoint, authenticate as that company to access its invoice data, and also obtain the victim's previous password verifier from the API response.	2026-08-24	7.1	CVE-2026-71505
dradis--dradis-ce	In Dradis Community Edition, the ProvidersController and AgentsController gate their admin_required before_action on `defined?(Dradis::Pro)`, a constant that is never defined in CE, so the authorization check is never applied. As a result, any authenticated (non-admin) user can create an AI provider pointing to an arbitrary HTTP/HTTPS address (including internal/link-local hosts such as http://169.254.169.254) and reassign the built-in Roslin agent to use it. When an AI interaction is triggered, the server issues a request to the attacker-supplied URL (server-side request forgery). For non-2xx responses, the target's response body is reflected verbatim to the attacker's browser via ActionCable/Turbo Stream error messages, making the SSRF readable.	2026-08-25	7.1	CVE-2026-79788
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the dray_apm component. The vulnerability is caused by insufficient validation of UDP message content after START_SPEED_TEST before command execution. A remote attacker can trigger this vulnerability via a crafted message to execute arbitrary commands with root privileges.	2026-08-24	9.8	CVE-2026-71914
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the tr069TestInform function. The vulnerability is caused by insufficient filtering of dangerous characters before the event_code field is concatenated into a system command. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71904
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the ExportSettings function. The vulnerability is caused by insufficient filtering of the backupkey, backuptype, and realtime fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71905
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the setLan function. The vulnerability is caused by insufficient validation of the lanIp and lanNetmask fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root	2026-08-24	7.2	CVE-2026-71906

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileges. Exploitation requires valid administrative credentials for the device's web management interface.			
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the setcamset function. The vulnerability is caused by insufficient filtering of the selectSlaves field before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71907
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the mesh_start_speed_test function. The vulnerability is caused by insufficient sanitization of the meshdevice_index and meshdevice_ip fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71908
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the InquirerTime function. The vulnerability is caused by insufficient filtering of the time field before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71909
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the apautotest function. The vulnerability is caused by insufficient validation of the CMD0, CMD3, and CMD6 fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71910
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a buffer overflow vulnerability in the setLan function. The vulnerability is caused by missing length checks during memory copy operations involving the lanVlanId0, lanIp, and lanNetmask fields. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71911
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a buffer overflow vulnerability in the apautotest function. The vulnerability is caused by missing length checks during memory copy operations involving the CMD6 field. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71912
DrayTek Corporation--VigorAP 918R	Multiple DrayTek VigorAP models contain a command injection vulnerability in the upload_settings.cgi interface. The vulnerability is caused by insufficient filtering before the restorekey field is concatenated into a shell command. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71913
DrayTek Corporation--VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a pre-authentication command injection vulnerability in the setget.cgi interface. The vulnerability is caused by insufficient filtering of the pass field before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges.	2026-08-24	9.8	CVE-2026-71921
DrayTek Corporation--VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain unauthorized operation vulnerabilities in multiple syslog functions. The vulnerability is caused by missing authorization checks. A remote attacker can trigger these vulnerabilities via crafted requests to modify configuration, restart services, save startup configuration, or clear logs.	2026-08-24	9.1	CVE-2026-71933
DrayTek Corporation--VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the jsonstatus function. The vulnerability is caused by insufficient filtering of the usescript, usefile, and option fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71915
DrayTek Corporation--VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the commandTable function. The vulnerability is caused by incomplete filtering of dangerous characters such as backticks, newline characters, and single quotes in the parameter field. A remote attacker can trigger this vulnerability via crafted	2026-08-24	7.2	CVE-2026-71916

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.			
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the pingtrace function. The vulnerability is caused by insufficient validation of the host field before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71917
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the webBackupAction function. The vulnerability is caused by insufficient filtering of the option, key, pw_encode, pathN, and valueN fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71918
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the sysreboot function. The vulnerability is caused by insufficient filtering of the config, act, pathN, and valueN fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71919
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a pre-authentication null pointer dereference vulnerability in the setget.cgi interface. The vulnerability is caused by missing validation when the pass field is absent. A remote attacker can trigger this vulnerability via a crafted request to crash the service and cause a denial of service.	2026-08-24	7.5	CVE-2026-71922
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the auth_set function. The vulnerability is caused by insufficient filtering of the username and password fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71923
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the getVid function. The vulnerability is caused by insufficient filtering of the username and password fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71924
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the getDetail function. The vulnerability is caused by insufficient filtering of the username and password fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71925
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the setDevice function. The vulnerability is caused by insufficient sanitization of the username, password, and location fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71926
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the rebDevice function. The vulnerability is caused by insufficient filtering of the username and password fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71927
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the fdftDevice function. The vulnerability is caused by insufficient filtering of the username and password fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71928
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the setDevProto function. The vulnerability is caused by insufficient filtering of the username and password fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root	2026-08-24	7.2	CVE-2026-71929

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileges. Exploitation requires valid administrative credentials for the device's web management interface.			
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the setTime function. The vulnerability is caused by insufficient filtering of the username and password fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71930
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the tftp_upgrade function. The vulnerability is caused by insufficient filtering before the filename field is concatenated into a command. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71931
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the pingtrace function. The vulnerability is caused by missing length checks when the host, count, and interval fields are concatenated into a fixed-size buffer. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71934
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the webBackupAction function. The vulnerability is caused by repeated string concatenation of the pathN, valueN, key, and option fields into fixed-size stack buffers without total length checks. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71935
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the sysreboot function. The vulnerability is caused by unsafe concatenation of split valueN data into a fixed-size buffer. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71936
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the poe_schedule_profile function. The vulnerability is caused by repeated concatenation of the start_date, start_time, duration_time, how_often, weekdays, monthly_date, and cycle_duration fields into small fixed-size buffers without proper length checks. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71937
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the switch_lan_gvrp function. The vulnerability is caused by unsafe copying of the portList field into an undersized buffer. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71938
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the acl_general_setup Add ACE function. The vulnerability is caused by copying the name field into a fixed-size buffer without length validation. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71939
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the acl_general_setup Edit ACE function. The vulnerability is caused by copying the name field into a fixed-size buffer without length validation. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71940
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the diag_logmail function. The vulnerability is caused by concatenating multiple smtpReceiver email addresses into a fixed-size buffer without checking the remaining buffer size. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands.	2026-08-24	7.2	CVE-2026-71941

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exploitation requires valid administrative credentials for the device's web management interface.			
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a buffer overflow vulnerability in the mail_mailalert function. The vulnerability is caused by concatenating multiple smtpReceiver email addresses into a fixed-size buffer without checking the remaining buffer size. A remote attacker can trigger this vulnerability via crafted input, causing a denial of service or potentially executing arbitrary commands. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71942
DrayTek Corporation-- VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a command injection vulnerability in the setDevNet function. The vulnerability is caused by insufficient filtering of the username and password fields before command execution. A remote attacker can trigger this vulnerability via crafted input to execute arbitrary commands with root privileges. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	7.2	CVE-2026-71943
Ebyte--Ebyte NE2-D11 Firmware	MQTT credentials and control traffic are transmitted in cleartext, exposing sensitive information to network-level attackers. This may enable unauthorized device impersonation and disruption of messaging functions.	2026-08-27	9.8	CVE-2026-69658
Ebyte--Ebyte NE2-D11 Firmware	The Ebyte device relies on client side authentication logic that can be reproduced by unauthenticated users. An attacker may generate valid authentication requests and bypass authentication to obtain administrative access to the device.	2026-08-27	9.8	CVE-2026-71187
Ebyte--Ebyte NE2-D11 Firmware	Ebyte device web management interface does not consistently enforce authentication before granting access to administrative functionality. An unauthenticated remote attacker could access sensitive configuration information, modify device settings, or disrupt availability.	2026-08-27	9.8	CVE-2026-73125
Ebyte--Ebyte NE2-D11 Firmware	An improper protection of authentication tokens vulnerability exists in certain Ebyte gateway products. Authentication tokens used by the web management interface are insufficiently protected during client-side session handling, which may allow an attacker with access to exposed session information to obtain and reuse a valid token. Successful exploitation could allow an attacker to impersonate an authenticated user and gain unauthorized access to device management functionality.	2026-08-27	9.8	CVE-2026-76179
Ebyte--Ebyte NE2-D11 Firmware	The Ebyte device does not adequately verify the origin or authenticity of requests submitted to the web management interface. An unauthenticated remote attacker could persuade an authenticated administrator to visit a crafted page, causing unauthorized configuration changes or a disruption of device availability.	2026-08-27	8.8	CVE-2026-75814
Ebyte--Ebyte NE2-D11 Firmware	Ebyte gateway product's vendor configuration utility does not require authentication before allowing certain disruptive administrative actions when default credentials remain configured. An unauthenticated attacker on the adjacent network could reboot the device or restore factory settings, resulting in a loss of configuration and service availability.	2026-08-27	8.1	CVE-2026-77977
Ebyte--Ebyte NE2-D11 Firmware	A cleartext transmission of sensitive information vulnerability exists in certain Ebyte gateway products. The web management interface does not adequately protect sensitive communications using transport-layer encryption. An attacker with access to network traffic could intercept authentication or session-related information transmitted between a user and the affected device. Successful exploitation could result in disclosure of sensitive information and unauthorized access to device management functionality.	2026-08-27	7.5	CVE-2026-73809
Ebyte--Ebyte NE2-D11 Firmware	Certain configuration endpoints may lack proper server-side authorization checks, allowing unauthorized users to access or modify sensitive device settings. This could result in full compromise of device functionality.	2026-08-27	7.5	CVE-2026-75813
Ebyte--Ebyte NE2-D11 Firmware	The affected Ebyte device does not restrict repeated authentication attempts through rate limiting or account lockout mechanisms. This could allow an attacker to perform automated authentication attacks against deployments that rely on password based authentication.	2026-08-27	7.5	CVE-2026-76940
Ebyte--Ebyte NE2-D11 Firmware	The affected Ebyte device relies on client-managed authentication tokens without sufficient server-side validation. An attacker may replay or manipulate authentication tokens to gain unauthorized access to administrative functionality.	2026-08-27	7.5	CVE-2026-76945
Edge-Themes-- Shuffle	The Shuffle theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.8. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2026-08-25	8.1	CVE-2026-78566

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
EFM--ipTIME T16000M	A weakness has been identified in EFM ipTIME T16000M 14.20.2. The impacted element is the function httpcon_check_session_url of the component Session Validation Handler. This manipulation causes improper authentication. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-24	10	CVE-2026-78167
EFM--ipTIME T24000M	A security vulnerability has been detected in EFM ipTIME T24000M up to 14.20.0. This affects the function httpcon_check_session_url of the component Session Validation Handler. Such manipulation leads to improper authentication. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-24	9.8	CVE-2026-78168
Elated-Themes--Mane	The Mane theme for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.7. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.	2026-08-25	8.1	CVE-2026-78478
Elated-Themes--Mne	Unauthenticated Local File Inclusion in MÃfÃ¥ne <= 1.7 versions.	2026-08-24	8.1	CVE-2026-66670
Elated-Themes--Verdure Core	Unauthenticated Local File Inclusion in Verdure Core <= 1.2 versions.	2026-08-24	8.1	CVE-2026-66671
emrevona--WP Fastest Cache WordPress Cache Plugin	The WP Fastest Cache - WordPress Cache Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via HTTP Host Header in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This requires the Polylang or Polylang Pro plugin to be active and the Combine JS option to be enabled, as these conditions trigger the vulnerable Host-header-to-URL code path that writes attacker-controlled script src values into the shared page-cache file served to all subsequent visitors.	2026-08-26	7.2	CVE-2026-19760
eosphoros-ai--DB-GPT	DB-GPT builds the destination path for an uploaded skill from the multipart filename without constraining it to the upload directory. skill_upload in packages/dbgpt-app/src/dbgpt_app/openapi/api_v1/agentica_data_api.py takes file.filename as given and writes the request body to upload_dir / filename. A path composed with that operator discards the left operand when the right one is absolute and follows parent references otherwise, so a filename such as ../../tmp/x or /tmp/x resolves outside the intended directory; nothing canonicalises the result, checks that it remains under the upload root, or prevents a .py suffix. The route's only dependency is get_user_from_headers in dbgpt_serve/utis/auth.py, which returns a request carrying the admin role whether or not a user_id header is supplied, so the endpoint is reachable without credentials. A remote attacker holding no account can therefore write attacker-controlled bytes to any path the server process can write, place a new Python module inside the application package or replace one the application already imports, and obtain code execution in the server process when that module is next imported.	2026-08-25	9.8	CVE-2026-80104
ePayco--Epayco	Unauthenticated SQL Injection in Epayco <= 8.4.6 versions.	2026-08-27	9.3	CVE-2026-78260
exceljs--exceljs	exceljs through 4.4.0 contains a prototype pollution vulnerability in the deepMerge helper that fails to reject __proto__, constructor, or prototype keys when merging note objects. Attackers can assign parsed JSON with a malicious __proto__ property to cell notes, modifying Object.prototype and affecting all plain objects created in the process.	2026-08-24	9.4	CVE-2026-78207
exceljs--exceljs	exceljs through 4.4.0 fails to neutralize leading equals, plus, minus, or at signs in cell values written to CSV output. Attackers who can influence exported cell values can inject formulas that execute when the CSV file is opened in a spreadsheet application, potentially exfiltrating data or performing other malicious actions.	2026-08-24	8.2	CVE-2026-78209
exceljs--exceljs	exceljs through 4.4.0 decompresses all entries from supplied xlsx archives into memory without limits on entry size, total size, or compression ratio. Attackers can upload highly compressed workbooks that expand to gigabytes in memory, exhausting available resources and causing denial of service.	2026-08-24	7.5	CVE-2026-78206
exceljs--exceljs	exceljs through 4.4.0 contains a path traversal vulnerability in the Workbook.addImage() function that fails to validate file paths. Attackers can supply	2026-08-24	7.5	CVE-2026-78208

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary file paths to read any file accessible to the Node.js process and embed it in the generated workbook.			
Extend Themes--Lead Generation Contact Widget & AI Chatbot: Chat Button, Phone Call, Telegram, Email SiteLeads	Unauthenticated Sensitive Data Exposure in Lead Generation Contact Widget & AI Chatbot: Chat Button, Phone Call, Telegram, Email - SiteLeads <= 1.2.0 versions.	2026-08-24	7.5	CVE-2026-78268
fast-uri--fast-uri	fast-uri is a URI parser for Node.js. It decodes percent escapes in a hostname during parsing and then decodes the parsed hostname a second time during authority recomposition, so a single call to normalize or resolve can turn nested percent-encoded input into a different network destination such as a loopback hostname or address. For example, a doubly encoded host that spells out a loopback name decodes to that live host in one operation, which contradicts RFC 3986 section 2.4 that an implementation must not decode the same string more than once. An application that normalizes or resolves an untrusted HTTP-family URI before outbound routing, redirect validation, or a host-policy check can receive a destination different from the one the original encoded host represented, giving a server-side request forgery and host-policy bypass primitive. This is an incomplete-fix variant of CVE-2026-6322. The affected versions are 2.4.1 up to but not including 2.4.5, 3.1.2 up to but not including 3.1.6, and 4.0.0 up to but not including 4.1.3. The issue is fixed in 2.4.5, 3.1.6, and 4.1.3, which normalize percent escapes once and preserve encoded percent signs. Users should upgrade to a patched version.	2026-08-24	7.5	CVE-2026-75899
fast-uri--fast-uri	fast-uri is a URI parser for Node.js. It canonicalizes a host to its ASCII form only when the input carries an explicit scheme, so a scheme-relative reference such as a host preceded by two slashes is returned with its host verbatim and no error set. As a result fast-uri's own entry points disagree with each other: parse, resolve, normalize, and equal can yield different hosts for the same input depending only on whether a scheme is written out, and equal can return opposite verdicts for the same pair of hosts. An application that extracts a host with fast-uri to check it against a policy list and then resolves the same reference can make its decision on one host while the destination is another, enabling host confusion and policy bypass. The affected versions are 2.4.2 up to but not including 2.4.5, 3.1.3 up to but not including 3.1.6, and 4.0.1 up to but not including 4.1.3. The issue is fixed in 2.4.5, 3.1.6, and 4.1.3, which canonicalize the host consistently across the resolve path. Users should upgrade to a patched version.	2026-08-24	7.5	CVE-2026-75931
fast-uri--fast-uri	fast-uri is a URI parser for Node.js. Its custom parser for bracketed IPv6 literals does not validate the complete IPv6 grammar, so invalid trailing text in an authority can be silently discarded and a malformed attacker-controlled host is turned into a different valid IPv6 destination. For example, a bracketed literal with invalid trailing characters is normalized to the unspecified address, which a Node HTTP client then connects to a local service over loopback, and other malformed literals collapse to private-range addresses. No error is set on the parsed result, so an application checking the error field cannot detect the rewrite. An application that normalizes untrusted URLs before outbound requests, redirects, proxy routing, or address-policy enforcement can be redirected to a local or private IPv6 target, giving a server-side request forgery and address-policy bypass primitive. The affected versions are 2.3.1 up to but not including 2.4.5, 3.0.0 up to but not including 3.1.6, and 4.0.0 up to but not including 4.1.3. The issue is fixed in 2.4.5, 3.1.6, and 4.1.3, which validate bracketed IP literals against the full grammar and mark malformed literals as authority errors. Users should upgrade to a patched version.	2026-08-24	7.5	CVE-2026-75975
fast-uri--fast-uri	fast-uri is a URI parser for Node.js. During parsing it runs a legacy decoding pass over the scheme component and never re-escapes the result, and serialization writes the scheme back out verbatim, unlike the host component which is re-escaped. As a result an input whose scheme carries percent-encoded slashes parses as a scheme with no authority, so the parsed host and error are both undefined, yet resolving or normalizing that same input emits a network-path reference whose authority is attacker-chosen and re-parses to that host. An application that allowlists on the parsed host, or treats a reference with no authority as safe to resolve against its base, gets the opposite of what it checked, giving an off-site redirect, server-side request forgery, or address-policy bypass. The legacy decoder also expands non-standard escape forms, widening the issue	2026-08-24	7.5	CVE-2026-76172

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	past upstream filters, and control characters in the scheme can reach the output as raw carriage return and line feed. The affected versions are 2.3.1 up to but not including 2.4.5, 3.0.0 up to but not including 3.1.6, and 4.0.0 up to but not including 4.1.3. The issue is fixed in 2.4.5, 3.1.6, and 4.1.3, which reject a scheme that is not valid after decoding. Users should upgrade to a patched version.			
Fdaws--node-poppler	A vulnerability was detected in Fdaws node-poppler up to 9.1.2/10.0.1. The impacted element is the function pdfInfo/pdfToText/pdfToCairo/pdfToPpm/pdfImages/pdfToHtml/pdfToPs/pdfFont s/pdfDetach/pdfAttach/pdfSeparate/pdfUnite of the file src/index.js of the component Argument Injection Handler. Performing a manipulation of the argument file_path results in argument injection. The attack may be initiated remotely. The patch is named db6e3f79d3beb20601be7e59669c39811ae3c330. It is recommended to apply a patch to fix this issue.	2026-08-25	7.3	CVE-2026-78637
filamentphp--filament	Filament is a collection of full-stack components for accelerated Laravel development. Prior to versions 4.12.0 and 5.7.0, incorrect challenge-form required-field handling allows app-based multi-factor authentication to be bypassed when recovery codes are enabled. Email-based multi-factor authentication is not affected. This issue is fixed in versions 4.12.0 and 5.7.0.	2026-08-24	8.1	CVE-2026-77567
flairNLP--flair	The official Flair wheels for 0.15.0 and 0.15.1 still contain flair/models/clustering.py, whose ClusteringModel.load static method returns pickle.loads(joblib.load(str(model_file))) and so executes arbitrary Python while loading a model file. Loading a model supplied by an attacker therefore runs that attacker's code with the privileges of the loading process. This is the same sink and the same file as CVE-2024-10073, which records 0.15.0 as the fixed version on the basis that clustering support was dropped in that release; the module was removed from the documented API but remains present in the distributed artifact and reachable by importing flair.models.clustering directly, so the earlier record's fixed version does not hold for the shipped package.	2026-08-24	7.8	CVE-2026-76843
Franky--Events Made Easy	Unauthenticated Cross Site Scripting (XSS) in Events Made Easy <= 3.2.5 versions.	2026-08-24	7.1	CVE-2026-28162
free5gc--free5gc	free5GC is an open-source implementation of the 5G core network. In version 1.4.4 and earlier, the AUSF component stores per-subscriber authentication state in a global sync.Map named AUSFContext.UePool in internal/context/context.go, keyed only by SUPI. Every request handled by internal/sbi/processor/ue_authentication.go creates an AusfUeContext, and AddAusfUeContextToPool executes ausfContext.UePool.Store(ausfUeContext.Supi, ausfUeContext), unconditionally replacing the active context for that SUPI. An attacker with access to the AUSF SBI/N12 interface can send concurrent POST /nausf-auth/v1/ue-authentications requests for the same target SUPI, causing all attempts to share one logical authentication context URL while K_aut, XRES, and EapID are repeatedly overwritten. A valid EAP-AKA' response for an earlier challenge is then checked against the latest context, causing AT_MAC verification to fail and denying authentication to the selected subscriber while the request flood continues. No fixed version is available as of this review.	2026-08-28	7.5	CVE-2026-55784
FURUNO ELECTRIC CO., LTD.--FA-50	FA-50 all versions contain hard-coded credentials. An attacker, who knows the credentials and has access to the vessel's internal network, can operate the settings screen using that credentials to alter the identification number.	2026-08-25	9.1	CVE-2026-59769
FURUNO ELECTRIC CO., LTD.--FA-50	FA-50 all versions miss authentication for some configuration. An attacker with access to the vessel's internal network can manipulate the product's settings screen to alter some configuration parameters.	2026-08-25	7.5	CVE-2026-67578
gemelo-ai--vocos	Vocos instantiates a class named by a configuration file without restricting which class may be named. instantiate_class in vocos/pretrained.py takes the class_path value from the configuration, splits it into a module and an attribute, imports the module with __import__, resolves the attribute with getattr, and calls the result as args_class(*args, **kwargs) where kwargs is the config's own init_args mapping. No allowlist constrains the dotted path, so a configuration may name any importable callable and supply the arguments it is called with. Vocos.from_hparams reaches this for each of the feature_extractor, backbone and head entries, and Vocos.from_pretrained reaches it with a remote file: it downloads config.yaml from a caller-named Hugging Face repository and passes it straight to from_hparams. Loading a model from a repository the user does not control therefore executes code of the repository owner's choosing in the loading process. The neighbouring torch.load of the downloaded weights is a separate	2026-08-25	8.8	CVE-2026-79784

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	matter and is constrained on PyTorch releases that default weights_only to true, which leaves this path as the reachable one.			
Genetec Inc.-- Synergis Softwire	Improper access control to the Synergis Softwire installation folder. This vulnerability affects Streamvault all-in-one appliances (SV-100E and SV-300E series) and Synergis Softwire installed on Windows servers.	2026-08-27	7.9	CVE-2026-44629
getgrav--grav	Grav Login plugin versions before 1.0.16 fail to validate the target account's privilege level in the onApiUserListRowAction unlock handler. An attacker with api.users.write permission can clear login lockout counters on admin.super accounts, removing brute-force protection from the highest-privilege accounts without requiring equivalent permissions.	2026-08-25	9.8	CVE-2026-56710
getgrav--grav	The getgrav/grav-plugin-api plugin before 1.0.18 does not enforce API-key scope in the requireNotSuperTarget() function in UsersController.php across seven sensitive user-management endpoints. The check uses isSuperAdmin() on the acting account rather than verifying whether the specific API key carries super authority (via isSuperWithinScope()). As a result, an API key scoped below full super authority but belonging to a super-admin account can act against other super-admin accounts- disabling their 2FA, deleting their avatar, minting new API keys under their identity, or deleting their existing API keys.	2026-08-26	9.8	CVE-2026-80203
getgrav--grav	Grav before 2.0.16 contains a path traversal vulnerability in MediaUploadTrait::deleteFile() that allows authenticated users with media management permissions to delete arbitrary files by supplying filenames with directory traversal sequences. The method validates only the basename portion of the filename while preserving unvalidated directory paths containing ../ sequences that are passed to unlink(), enabling deletion of files outside the intended media storage directory.	2026-08-25	8.1	CVE-2026-72695
getgrav--grav	Grav CMS before 2.0.16 contains a symlink following vulnerability in Scheduler Job::createLockFile() that allows local attackers to overwrite arbitrary files by pre-creating symlinks at predictable lock file paths in the world-writable temp directory. Attackers can place a symlink at the predictable lock path pointing to any file the web server process can write to, and the next scheduled job run will follow the symlink and overwrite the target file's content with the job ID string.	2026-08-25	8.4	CVE-2026-72696
getgrav--grav	The Grav Email plugin (getgrav/grav-plugin-email) before 4.2.2 renders page-editor-controlled Email action parameters as unsandboxed Twig templates. An authenticated remote user with only api.access and api.pages.write permissions can place a Twig expression in header.form.process.email.body, publish the page, and submit the form to execute an arbitrary operating-system command as the account running PHP.	2026-08-25	8.8	CVE-2026-75574
getgrav--grav	Grav Flex Objects plugin versions 1.4.0 through 1.4.7 contain an authorization bypass vulnerability in the flex-objects shortcode that allows users with page-edit access to render any registered Flex collection without permission checks. Attackers can place the shortcode in published pages to expose sensitive directory contents including user account information, bypassing the authorize ACL enforced in the admin panel.	2026-08-25	7.7	CVE-2026-56707
getgrav--grav	Grav before 3.9.2 fails to validate untrusted Host headers in the sendInvitationEmail() function when constructing token-bearing invitation links. Attackers can manipulate the Host header to poison invitation links and redirect users to attacker-controlled domains, bypassing the require_trusted_host protection which only covers password reset flows.	2026-08-25	7.5	CVE-2026-56709
getgrav--grav	The getgrav/grav-plugin-login Composer plugin before 3.9.1 (used by Grav) compares password reset and account activation tokens using a non-constant-time === string comparison instead of hash_equals() in classes/Controller.php (taskReset()) and login.php (activation handler). Because the token-submission endpoint (taskReset) also lacks rate limiting, an attacker could in principle send repeated token guesses against a known username and use the timing differences to attempt to recover a valid token, though the vendor rates the practical exploitability as low and no end-to-end network exploit has been demonstrated.	2026-08-25	7.5	CVE-2026-72700
getgrav--grav	Grav before 2.0.16 contains an incomplete default denylist in the Twig sandbox configuration that fails to block access to system configuration secrets. Attackers with page-edit permission can use config.get() or config.toArray() in Twig templates to retrieve sensitive values like system.cache.redis.password when config_access is enabled.	2026-08-25	7.5	CVE-2026-76846
GhostManager-- Ghostwriter	Ghostwriter before 7.1.2 fails to validate template ownership in the report template swap endpoint, allowing attackers to attach client-scoped templates from other clients to their own reports. Attackers can exploit sequential template	2026-08-24	7.1	CVE-2026-78203

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	primary keys to enumerate and attach foreign templates, then generate reports to disclose template contents including letterhead, boilerplate, and methodology text.			
Gitea--Gitea	Gitea before 1.27.1 allows remote code execution via the diffpatch API through Git hook installation.	2026-08-26	9.8	CVE-2026-60004
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 18.9 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user with developer-role permissions could have executed arbitrary commands in a CI context, due to the Claude agent processing configuration from a user-controlled source.	2026-08-26	7.3	CVE-2026-18252
GitLab--GitLab AI Gateway	GitLab has remediated a vulnerability in the GitLab AI Gateway component affecting all versions of the AI Gateway from 18.9.0 to 19.0.12, 19.1 to 19.1.7, and 19.2 to 19.2.2 that could have allowed an authenticated user with Duo Agent Platform access to redirect model requests to an externally-controlled endpoint via crafted model metadata, resulting in the disclosure of Google Vertex AI or AWS Bedrock cloud service credentials.	2026-08-27	8.2	CVE-2026-19889
GitLab--GitLab AI Gateway	GitLab has remediated a vulnerability in the GitLab AI Gateway component affecting all versions of the AI Gateway from 18.10 to 19.0.12, 19.1 to 19.1.7, and 19.2 to 19.2.2 that could have allowed an authenticated user with Duo Agent Platform access to redirect outbound model requests to an externally-controlled endpoint via a crafted inline flow configuration that overrides the HTTP Host header, resulting in disclosure of Google Cloud Vertex cloud service credentials and private signing keys.	2026-08-27	8.2	CVE-2026-75871
GitoxideLabs--gitoxide	gitoxide's gix-url crate (<= 0.32.0, fixed in 0.37.1) uses a hand-rolled URL parser that does not treat '?' or '#' as terminating the authority component, contrary to RFC 3986. As a consequence, gix-transport's HTTP redirect identity guard (can_reuse_identity) compares the wrong host and fails open. An attacker controlling a redirect response can craft a Location header of the form <attacker-authority>?@<original-authority> so that gitoxide sends the caller's HTTP Basic Authorization credentials to an unintended host. gix-transport is affected in versions <= 0.49.0 (fixed in 0.58.1).	2026-08-28	7.5	CVE-2026-82247
GitoxideLabs--gitoxide	gitoxide before 0.52.1 fails to validate submodule names from .gitmodules configuration, allowing path traversal when deriving submodule git directories. Attackers can craft malicious submodule names with traversal segments to redirect state() and open() functions to repositories outside .git/modules, causing repository confusion and inspection of attacker-controlled repositories.	2026-08-28	7.5	CVE-2026-82251
GitoxideLabs--gitoxide	gitoxide before 0.52.1 follows symlinks when reading the worktree .gitmodules file, allowing attackers to inject out-of-repository bytes into submodule metadata. Attackers can create a malicious repository with a symlinked .gitmodules pointing outside the repository tree, causing gitoxide to parse arbitrary external files as submodule configuration and expose attacker-controlled name, path, and url values.	2026-08-28	7.5	CVE-2026-82252
GitoxideLabs--gitoxide	gitoxide (Rust crates gix <= 0.72.0 and gix-validate <= 0.10.0) contains a path traversal vulnerability. The submodule name validation function in gix-validate only checks the first occurrence of '..' via name.find(b".."), allowing crafted names such as 'a..b/../../../../.git/' to bypass the check; additionally this validation is never invoked in production code paths. Combined with a trust inheritance flaw in Submodule::open(), where the parent repository's git_dir_trust (Trust::Full) is cloned and the ownership verification is skipped, an attacker can craft a malicious .gitmodules file so that a victim tool built on gitoxide reads arbitrary git repository configuration (including embedded credentials) with full trust, bypassing safe-directory protections. Fixed in gix 0.82.0 and gix-validate 0.11.1.	2026-08-28	7.5	CVE-2026-82253
GitoxideLabs--gitoxide	gitoxide before 0.69.0 contains unchecked array indexing in delta application and uncapped allocation from attacker-controlled size headers in gix-pack. Attackers can send crafted pack data during clone or fetch operations to trigger panics or out-of-memory process kills.	2026-08-28	7.5	CVE-2026-82254
gitpython-developers--GitPython	GitPython before 3.1.59 fails to safely re-serialize multi-line git-config values during write operations, corrupting dormant quoted values into injected directives like core.hooksPath. Attackers can craft config files with embedded newlines that become live git directives after any unrelated GitPython config write, enabling arbitrary code execution via hook invocation.	2026-08-25	9.8	CVE-2026-78676
gitpython-developers--GitPython	GitPython before 3.1.59 fails to disable merge_includes when parsing .gitmodules, allowing attackers to disclose local file content by including arbitrary file paths via [include] directives. Attackers can craft a malicious .gitmodules file with include	2026-08-25	8.4	CVE-2026-78675

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	directives pointing to sensitive files; when repo.submodules is accessed, GitConfigParser raises MissingSectionHeaderError embedding the target file's first line verbatim in the exception message.			
gitpython-developers--GitPython	GitPython before 3.1.59 omits --separate-git-dir from unsafe_git_clone_options, allowing attackers to create arbitrary git directories outside the intended clone destination. Attackers can pass a separate_git_dir parameter to Repo.clone_from() or Repo.clone() to redirect repository metadata to an attacker-controlled filesystem path, enabling arbitrary directory creation and potential hook execution.	2026-08-25	7.5	CVE-2026-78677
GNOME--Dia	A heap-based buffer overflow vulnerability exists in the Dia diagram editor WPG file format importer. In plug-ins/wpg/wpg-import.c, the WPG import renderer allocates a fixed palette with: ren->pPal = g_new0(WPGColorRGB, 256); When handling a WPG_COLORMAP record, the parser reads a start index (i16) and number of colors (iNum16) from the file and reads palette data with: bRet &= (iNum16 == (int)fread(&ren->pPal[i16], sizeof(WPGColorRGB), iNum16, f)); The only bounds-related check is `if (i16 >= 0 && i16 <= iSize)`, where iSize is the WPG record size-not the palette capacity. There is no validation that i16 is less than 256 or that i16 + iNum16 does not exceed 256. A malicious WPG file can supply i16=256 and iNum16=264. That causes fread() to write 792 bytes starting at &pPal[256], while the palette buffer is only 768 bytes (256 entries Ãƒ- 3 bytes). This overflows into adjacent heap metadata and can crash Dia (SIGABRT / malloc corruption errors) or, depending on heap layout and exploit primitives, potentially lead to arbitrary code execution. Exploitation requires convincing a user to open a crafted WPG file via Dia's file dialog, command line, or file association. No special privileges are required to deliver the file to the victim. Affected component: WPG parser (plug-ins/wpg/wpg-import.c). Affected versions: all Dia versions containing this code path (reporter tested Dia 0.98+git20260221-1; issue present on upstream master as of 2026-08-21).	2026-08-26	7.8	CVE-2026-77652
GNOME--Dia	A stack-based buffer overflow vulnerability exists in the Dia diagram editor when processing Network Bus objects from Dia XML project files. In objects/network/bus.c, bus_load() reads the number of bus handles from the file attribute "bus_handles" using attribute_num_data() without validating an upper bound: bus->num_handles = attribute_num_data(attr); When a bus handle is subsequently moved, bus_handle_moved() allocates two temporary arrays on the stack: parallel = (real *)g_alloca(num_handles * sizeof(real)); perp = (real *)g_alloca(num_handles * sizeof(real)); Because num_handles is fully attacker-controlled via the project file, sufficiently large values (for example 262144 or higher) cause g_alloca() to consume more stack space than the default thread stack limit (typically 8 MB on Linux), resulting in stack overflow, SIGSEGV, and potential stack frame / return-address corruption. An attacker can embed a Bus object with an excessive bus_handles count in a malicious .dia file. Exploitation requires the victim to open the file in Dia (file dialog, command line, or file association) and trigger handle manipulation (moving a bus handle), which exercises the vulnerable code path. The identical g_alloca pattern is present in objects/Misc/tree.c (copied from bus.c) and is likely vulnerable to the same class of attack via Tree objects. Affected versions: Dia 0.98.0 and earlier versions containing this code; issue confirmed on upstream master as of 2026-08-21. Upstream report: https://gitlab.gnome.org/GNOME/dia/-/issues/581	2026-08-26	7.8	CVE-2026-77658
GNOME--GIMP	A flaw was found in the file-pcx plugin in GIMP, affecting 32-bit builds only. When processing a PCX image file, the plugin calculates memory allocation sizes based on the image dimensions and the number of color planes. If a crafted file sets the number of planes to 4 alongside sufficiently large dimensions, the calculation exceeds the 32-bit integer limit and overflows, resulting in an undersized heap-based buffer allocation. This integer overflow issue results in a heap-based buffer overflow when the plugin subsequently writes image data into the undersized buffer, causing memory corruption, potentially leading to arbitrary code execution or a denial of service.	2026-08-24	7	CVE-2026-78465
go-vikunja--vikunja	Vikunja is an open-source self-hosted task management platform. From 0.24.6 until 2.4.0, DELETE /api/v1/projects/:project/views/:view permits an authenticated user to supply a view identifier from another project while authorizing only against an attacker-controlled project identifier. ProjectView.CanDelete in pkg/models/project_view_permissions.go does not establish that the view belongs to the path project, and ProjectView.Delete in pkg/models/project_view.go continues after the scoped project_views delete affects no rows. Its subsequent deletes select task_buckets and task_positions only by project_view_id, allowing	2026-08-28	8.1	CVE-2026-55065

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cross-tenant destruction of Kanban assignments and ordering while leaving the victim view and tasks intact. This issue is fixed in version 2.4.0.			
go-vikunja--vikunja	Vikunja is an open-source self-hosted task management platform. Prior to 2.4.0, POST /api/v1/projects/{project}/views/{view}/buckets/{bucket}/tasks accepts a body supplied task_id but TaskBucket.CanUpdate in pkg/models/kanban_task_bucket.go authorizes only the project, view, and bucket from the URL. updateTaskBucket then calls Task.ReadOne without a separate task permission check, returns the victim task contents, and can update the task done state when the attacker chooses a done bucket. Because task identifiers are global sequential values, an authenticated user can enumerate cross-tenant tasks and modify their completion metadata through both the v1 and v2 routes that share this model. This issue is fixed in version 2.4.0.	2026-08-28	7.1	CVE-2026-55066
gohugoio--hugo	Hugo's security.http.urls allowlist is the only control on outbound fetches made by resources.GetRemote, and it inspects the URL text alone. CheckAllowedHTTPURL in config/security/securityConfig.go applies the configured pattern list and then re-checks a canonicalised form of an integer, hex or octal IPv4 host, but it never resolves the hostname and never inspects the address the HTTP client actually connects to. The client constructed in resources/resource_factories/create/create.go installs no dial-time hook, so no check occurs at connection time either. A hostname that resolves to a loopback, private or cloud-metadata address therefore satisfies the policy, and the response body is embedded in the generated site. An attacker who can supply a URL through content, for example a front-matter field or a CMS field, can make the build fetch an internal endpoint and publish the response in the static output, so the build artifact itself carries the data out.	2026-08-24	7.4	CVE-2026-10582
GoodLayers--Tourmaster	Unauthenticated Cross Site Scripting (XSS) in Tourmaster <= 5.4.9 versions.	2026-08-24	7.1	CVE-2026-28166
gophish--gophish	Gophish through 0.12.1 fails to enforce account lockout and password change requirements in the API authentication middleware. Attackers with valid API keys can bypass these security controls and retain full API access even when their account is locked or password change is required.	2026-08-28	8.1	CVE-2026-82269
GOVCERT-LU--eml_parser	eml_parser serves as a python module for parsing eml files and returning various information found in the e-mail as well as computed information. Prior to 3.0.2, eml_parser.routing.noparenthesis in eml_parser/routing.py removes parenthesized CFWS comments from Received: headers with a regex-based fix-point loop whose running time is quadratic in the nesting depth. A single Received: header with 5,000 nested parentheses causes approximately 1.3 seconds of CPU saturation per parsed message, and doubling the nesting depth approximately quadruples the running time. An attacker can submit relatively small EML files that consume multiple seconds of processing time, causing worker latency, queue backpressure, and possible service-level outages in synchronous gateways, sandboxes, and real-time triage pipelines. This issue is fixed in version 3.0.2.	2026-08-25	7.5	CVE-2026-55620
GoWind--go-wind-cms	go-wind-cms (GoWind) before 1.0.0 has a missing authorization vulnerability. The NewAuthorizer() function in app/admin/service/internal/data/data.go and app/app/service/internal/data/data.go returns a no-op authorization engine (noop.State{}), so the authz middleware always allows requests. Any authenticated user (regardless of role or tenant) can invoke administrative APIs such as deleting users, resetting passwords, and creating tenants.	2026-08-27	8.8	CVE-2026-75419
Grafana--Alloy	Grafana Alloy's prometheus.operator.servicemonitors component allows a user who can create or modify ServiceMonitor resources in a watched namespace to specify an arbitrary local file through bearerTokenFile. Alloy reads the file and sends its contents as a bearer token to an attacker-controlled scrape endpoint. This may disclose files accessible to the Alloy process, including its projected Kubernetes service account token, potentially granting the attacker Alloy's Kubernetes permissions. Exploitation requires ServiceMonitor write access and lower privileges than Alloy's service account.	2026-08-27	7.7	CVE-2026-75889
Graylog2--graylog2-server	Graylog is a free and open log management platform. Prior to Graylog Server versions 6.3.12, 7.0.7, and 7.1.2 and Graylog Forwarder version 7.3, the FortiGate key-value syslog parser in graylog2-server/src/main/java/org/graylog2/inputs/codecs/GLFortiGateSyslogEvent.java and graylog2-server/src/main/java/org/graylog2/inputs/codecs/SyslogCodec.java mishandles field-like text inside quoted values. GLFortiGateSyslogEvent.getFields() uses KV_PATTERN and QUOTED_KV_PATTERN, while SyslogCodec.parse() invokes the FortiGateSyslogEvent parser; crafted values containing = or backslash-escaped	2026-08-28	7.5	CVE-2026-55841

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	quotes can cause embedded keys such as srcip, dstip, date, time, and tz to remove or overwrite original top-level fields or produce an invalid message that Graylog discards. An unauthenticated network sender who can submit syslog messages can therefore manipulate security-log fields or evade logging to obscure malicious activity. This issue is fixed in Graylog Server versions 6.3.12, 7.0.7, and 7.1.2 and Graylog Forwarder version 7.3.			
Green-Computing--NUMail	NUMail developed by Green-Computing has an OS Command Injection vulnerability. Unauthenticated remote attackers can inject arbitrary OS commands and execute them on the server.	2026-08-28	9.8	CVE-2026-82082
Greenbone--Greenbone OS	A remote attacker with user privileges may use a malicious or compromised NASL vulnerability test (VT) on the affected products to trigger a stack buffer overflow and gain full access on the compromised system.	2026-08-27	8.8	CVE-2026-81625
GROWI, Inc.--GROWI	GROWI applies its page-viewer permission check to attachment requests only when the request carries an authenticated user. retrieveAttachmentFromIdParam in apps/app/src/server/routes/attachment/get.ts guards the check with a condition requiring the user to be non-null, so a request that carries no session skips the check entirely and the handler returns the file. The routes reached this way, /attachment/:id and /download/:id, take the attachment identifier from the path, so an unauthenticated caller who has an attachment identifier receives the file regardless of whether the page owning it is private and regardless of whether that caller would be permitted to view the page. Identifiers can be retained by a user whose access was later removed, or recovered from anywhere the identifier was previously exposed. Version 8.0.2 runs the check for authenticated and unauthenticated requests alike, skipping it only where a valid share link has already bound the requested file to that link's page.	2026-08-25	7.5	CVE-2026-80191
guno1928--alos-http	ALOS HTTP is a Linux-first Go web framework and application server built around a custom networking stack. Prior to 0.0.0-20260617230736-314b6783e196, core/utls.go::sanitizeRequestPath calls splitPathQuery on a request path beginning with a question mark and then performs the unchecked p[0] access without checking whether the resulting path is empty. An unauthenticated client can send a malformed request such as a question-mark-only path through h1_plain.go::ParseH1RequestHead, hpack.go::decodeSimpleGetPathHTTPSRequest, hpack.go::observeHeader, or h3_conn.go::handleRequestStream, causing an out-of-bounds panic before core.Recovery() middleware runs and terminating the server process. This issue is fixed in pseudo-version 0.0.0-20260617230736-314b6783e196.	2026-08-28	7.5	CVE-2026-55484
hashtemes--Hash Form	Unauthenticated PHP Object Injection in Hash Form <= 1.4.1 versions.	2026-08-27	9.8	CVE-2026-78292
hbs--hbs	hbs is an Express view engine that wraps Handlebars. Its registerAsyncHelper API bypasses Handlebars' automatic HTML escaping: an async helper returns an opaque placeholder during the first render pass, so the double-brace expression escapes only the placeholder, and after rendering hbs substitutes the placeholder with the raw callback return value without escaping it, across the cached, uncached, and layout render paths. An application that passes attacker-influenced data, for example user-supplied content from a database, into an async helper callback can therefore have arbitrary HTML and JavaScript injected into the server-rendered page, resulting in stored or reflected cross-site scripting. Versions 2.1.0 through 4.2.1 are affected, and the issue is fixed in 4.3.0, which HTML-escapes async helper output. Applications that intentionally emit raw HTML from an async helper can opt in explicitly with hbs.SafeString. Users should upgrade to 4.3.0.	2026-08-25	8.1	CVE-2026-16231
HCLSoftware--HCL Hive	HCL Hive is affected by incorrect default permissions which could allow an attacker unauthorized lateral movement, container breakout, and interception of sensitive internal communications.	2026-08-24	7.5	CVE-2025-68825
HCLSoftware--HCL Hive	HCL Hive is affected by a cryptographic primitive with a risky implementation which could allow an attacker unauthorized lateral compromise or widespread credential leakage if a single internal component is breached.	2026-08-24	7.4	CVE-2026-21751
HCLSoftware--HCL Hive	HCL Hive is affected by a use of vulnerable third-party components which could allow an attacker unauthorized access or compromise of the system by exploiting publicly documented security flaws.	2026-08-24	7.5	CVE-2026-21752
HCLSoftware--HCL Hive	HCL Hive is affected by a broken access control vulnerability which could allow an attacker or unauthorized user to introduce unverified, malicious, or broken code directly into production environments.	2026-08-24	7.2	CVE-2026-21756
Hepta Platforms--Heptabase	Heptabase developed by Hepta Platforms, Inc. has a Stored Cross-Site Scripting vulnerability. Authenticated remote attackers can inject persistent malicious	2026-08-24	8.7	CVE-2026-78213

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	content into specific pages, causing arbitrary JavaScript code to execute when other users click the crafted content.			
heyform--heyform	HeyForm before 3.0.0-rc.8 reflects the request Origin header in CORS responses while allowing credentials, enabling cross-origin requests with authentication. Attackers can execute authenticated GraphQL queries from malicious pages visited by logged-in users to access workspaces, projects, forms, submissions, and respondent data, or modify account settings.	2026-08-28	8.1	CVE-2026-82291
HiEventsDev--Hi.Events	Hi.Events validates a webhook destination only when it is registered, never when it is used. NoInternalUrlRule in backend/app/Validators/Rules/NoInternalUrlRule.php resolves the hostname with gethostbyname() and rejects private and reserved ranges, which any public hostname passes. At dispatch, WebhookDispatchService takes the stored URL and calls it through spatie/laravel-webhook-server without repeating the check, and backend/config/webhook-server.php sets no Guzzle options, so redirect following remains enabled by default. A destination that answers with a redirect to a loopback, private or cloud metadata address therefore causes the server to issue that request, and changing the hostname's DNS record after registration reaches the same result because no resolution is repeated. The response is not discarded: WebhookResponseHandlerService stores the body on the webhook log and WebhookLogResource returns it from the webhook logs endpoint, so the requester reads what the internal service replied rather than inferring it. Both event and organizer webhooks share the rule and the dispatch path. Version 1.11.1-beta revalidates at dispatch, pins the validated address, checks every redirect hop, and decodes IPv6 transition addresses that previously bypassed the filter.	2026-08-24	8.5	CVE-2026-76838
HumanSignal--label-studio	Label Studio does not scope the annotation detail endpoint to the requesting user's organization. AnnotationAPI in label_studio/tasks/api.py declares queryset = Annotation.objects.all() and provides no get_queryset override, so the default lookup retrieves any annotation by primary key. The view's permission_required entries name annotations.view, annotations.change and annotations.delete, and label_studio/core/permissions.py registers every permission with rules.is_authenticated, so the check is satisfied by any logged-in account and no object-level organization test runs. The sibling task endpoint does constrain its queryset with project__organization set to the requester's active organization, which is the boundary this path omits. Annotation identifiers are sequential integers, so an authenticated user of one organization can enumerate identifiers to read, modify and delete annotations belonging to other organizations on the same instance. The same unscoped queryset appears on AnnotationConvertAPI in the same file.	2026-08-24	8.8	CVE-2026-76073
hyperdxio--hyperdx	HyperDX through 1.10.1 fails to enforce role-based access controls in team management endpoints, allowing any team member to perform administrative actions. Attackers can delete team members including owners, rotate API keys, and rename teams by sending requests to PATCH /team/apiKey, PATCH /team/name, and DELETE /team/member endpoints.	2026-08-28	8.1	CVE-2026-82279
IBM--Administration Runtime Expert for i	IBM Administration Runtime Expert for i 1R1M0 IBM Application Runtime Expert (ARE) for i could allow a remote attacker to gain elevated privileges, caused by ARE GUI component processing. An unauthenticated attacker can exploit this vulnerability to execute actions under another user's authenticated profile gaining elevated privileges on the IBM i system.	2026-08-28	9.9	CVE-2026-18527
IBM--Administration Runtime Expert for i	IBM Administration Runtime Expert for i 1R1M0 could allow a remote authenticated attacker to obtain sensitive information due to improper authentication enforcement.	2026-08-28	7.5	CVE-2026-17203
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to gain elevated privileges due to a format string vulnerability.	2026-08-28	7	CVE-2026-16821
IBM--Concert	IBM Concert 1.0.0 through 2.3.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2026-08-28	9.1	CVE-2026-3627
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote attacker to execute arbitrary code due to improper enforcement of security restrictions on the A2A public endpoint.	2026-08-28	9.8	CVE-2026-19286
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.11.1 allows an authenticated attacker to execute arbitrary operating system commands in the server process by saving a flow with a crafted type field value and triggering a build of a wrapper flow that references it. This allowed privilege escalation from "authenticated flow user" to	2026-08-28	9.9	CVE-2026-19295

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary OS-level command execution under the server process identity, bypassing the LANGFLOW_ALLOW_CUSTOM_COMPONENTS=false policy control.			
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote authenticated attacker to execute arbitrary code due to improper control of generation of code.	2026-08-28	8.8	CVE-2026-18729
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote attacker to execute arbitrary flows and access sensitive information due to improper authentication.	2026-08-28	8.2	CVE-2026-18891
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote attacker to obtain sensitive information and inject unauthorized messages due to a namespace collision between user identifiers.	2026-08-28	8.2	CVE-2026-18904
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote attacker to read arbitrary files due to path traversal.	2026-08-28	7.5	CVE-2026-18899
idurar--idurar-erp-crm	IDURAR ERP CRM changes the password of whichever account a request names rather than the account making the request. The update handler in backend/src/controllers/middlewaresControllers/createUserController/updatePassword.js resolves the authenticated user from the request that the token middleware populated, then issues its update against a filter built from the identifier in the URL path, and never compares the two. The route is mounted behind the administrator token check only, so any valid administrator session is sufficient, and the sole ownership-like guard in the handler rejects a single hardcoded demo address. A caller can therefore set an arbitrary password on any other administrator account and sign in as it. The read handler in the same controller directory accepts an identifier the same way, which supplies the identifiers needed to pick a target.	2026-08-26	7.2	CVE-2026-81031
iflytek--astron-agent	iFlytek astron-agent through 1.1.1 contains an authorization bypass vulnerability in the copyFlow endpoint that fails to validate workflow ownership. Authenticated attackers can enumerate workflow identifiers and overwrite other tenants' workflows or copy private workflows to read their definitions.	2026-08-29	8.1	CVE-2026-82475
IGEL--IGEL OS 12	IGEL OS 12 before 12.7.6 and IGEL OS 11 before 11.11.150 contain a boot registry parameter injection vulnerability that allows attackers with physical access to execute arbitrary Linux loader parameters by writing to an unencrypted and unsigned configuration area read by the signed bootloader. Attackers can inject malicious kernel command line parameters that execute with boot environment privileges without triggering TPM PCR measurement failures, as the attack does not modify the measured boot code.	2026-08-28	7.6	CVE-2026-82017
ILIAS-eLearning e.V.--ILIAS	ILIAS deserialises stored session data for an unauthenticated caller. The Shibboleth back-channel endpoint at components/ILIAS/AuthShibboleth/resources/shib_logout.php runs in a context that ilInitialisation exempts from authentication, and its logout-notification handler locates the session to terminate by reading every live row of the session table and passing each row's stored data to a hand-written parser that calls unserialize without restricting which classes may be constructed. Any serialised object present in any session row is therefore instantiated on behalf of an anonymous request, and object destructors run when those objects are discarded. A serialised object can be placed into a session row without logging in, because the LTI authentication entry point stores request parameters into the session and is reachable on a path the same initialisation code exempts from authentication. A class bundled with the application writes a JSON-encoded structure to a file named by one of its own properties when it is destroyed, which places attacker-controlled content at an attacker-chosen path below the web root and results in code execution as the web server user. Versions 9.22, 10.10 and 11.3 remove the endpoint's logout-notification implementation.	2026-08-26	9.8	CVE-2026-80428
ilya-zlobintsev--LACT	Polkit Authentication Based on UnixProcessSubject / Peer PID in LACT on Linux allows an Authentication Bypass. This issue affects LACT through 0.10.0. Fixed by commit d0478fe42c2219454e272f96b1cbd29ab37ee566.	2026-08-25	7	CVE-2026-75037
INFINITUM FORM--Geo Controller	Unauthenticated PHP Object Injection in Geo Controller <= 8.9.8 versions.	2026-08-27	9.8	CVE-2026-78286
Infused Addons--InfusedWoo Pro	The InfusedWoo Pro plugin for WordPress is vulnerable to Privilege Escalation via Account Takeover in all versions up to, and including, 5.1.17. This is due to a missing capability check in the `ajax_iwar_preview_email()` function, which uses `is_admin()` as its only authorization check and allows low-privilege users to render email preview merge fields for an arbitrary email address. This makes it possible for authenticated attackers, with subscriber-level access and above, to generate and retrieve a valid password reset link for any WordPress user, including administrators, enabling account takeover.	2026-08-25	8.8	CVE-2026-19892

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Inisev--Social Media & Share Icons	Unauthenticated Cross Site Scripting (XSS) in Social Media & Share Icons <= 2.9.9 versions.	2026-08-24	7.1	CVE-2026-66623
iot-ecology--rust-iot-platform	rust-iot-platform through commit 5df942ab contains an authentication bypass vulnerability where most REST API routes lack authentication guards in their handler signatures. Unauthenticated attackers can create, update, list, retrieve, and delete user accounts by directly accessing unprotected endpoints without providing valid credentials.	2026-08-29	9.8	CVE-2026-82452
iot-ecology--rust-iot-platform	rust-iot-platform through commit 5df942ab stores user passwords in cleartext without hashing in the user model. Attackers can read API responses from user retrieval and listing routes to obtain plaintext credentials for all accounts.	2026-08-29	7.5	CVE-2026-82453
itsourcecode--Online Clinic Management System	A vulnerability has been found in itsourcecode Online Clinic Management System 1.0. This vulnerability affects unknown code of the file success/login.php of the component Admin Login. The manipulation of the argument Username leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2026-08-24	7.3	CVE-2026-78246
itsourcecode--Online Pharmacy System	A flaw has been found in itsourcecode Online Pharmacy System 1.0. This affects the function move_uploaded_file of the file all_users/register.php of the component User Registration. Executing a manipulation of the argument photo can lead to unrestricted upload. The attack may be launched remotely. The exploit has been published and may be used.	2026-08-24	7.3	CVE-2026-78245
itsourcecode--Payroll System	A vulnerability has been found in itsourcecode Payroll System 1.0. The impacted element is the function Login of the file admin_class.php. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2026-08-24	7.3	CVE-2026-78201
itsourcecode--Payroll System	A vulnerability was found in itsourcecode Payroll System 1.0. This affects the function save_settings of the file admin_class.php. The manipulation of the argument img results in unrestricted upload. The attack may be performed from remote. The exploit has been made public and could be used.	2026-08-24	7.3	CVE-2026-78202
itsourcecode--Payroll System	A flaw has been found in itsourcecode Payroll System 1.0. The impacted element is the function create/read/update/delete of the file ajax.php of the component CRUD Operation Handler. Executing a manipulation of the argument action can lead to missing authentication. The attack may be performed from remote. The exploit has been published and may be used.	2026-08-26	7.3	CVE-2026-81202
itsourcecode--Real Estate Management System	A vulnerability was detected in itsourcecode Real Estate Management System 1.0. Affected by this issue is some unknown functionality of the file search.php. Performing a manipulation of the argument search/delivery_type/search_price/property_type results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used.	2026-08-24	7.3	CVE-2026-78244
itsourcecode--Sales and Inventory System	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/processlogin.php. The manipulation of the argument User leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2026-08-24	7.3	CVE-2026-78171
ivolve--Customer Reviews for WooCommerce	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the aggregated review form submission in versions up to and including 5.106.0. This is due to insufficient input sanitization and output escaping on user-supplied review comment text. The plugin accepts review submissions from unauthenticated users through the 'cr_local_forms_submit' AJAX action without sanitizing HTML content before storing it via wp_insert_comment(), and later renders this stored content on product pages through comment_text() without proper escaping. This makes it possible for unauthenticated attackers with a valid review form URL (obtainable through review reminder emails sent to customers who placed orders) to inject arbitrary web scripts in pages that will execute whenever a user accesses the affected product page.	2026-08-28	7.2	CVE-2026-6176
izpack--izpack	IzPack is a widely used tool for packaging applications on the Java platform as cross-platform installers. In 5.2.6 and earlier, UnpackerBase.unpack() in izpack-installer/src/main/java/com/izforge/izpack/installer/unpacker/UnpackerBase.java obtains an attacker-controlled PackFile targetPath, passes it through IoHelper.translatePath(), which only converts separators, and constructs a File without normalizing parent-directory segments or enforcing destination containment. A malicious installer pack entry containing ../ sequences can therefore write outside the intended installation directory to startup folders,	2026-08-26	7.4	CVE-2026-54550

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	executable search paths, or other locations accessible with the victim's privileges when the victim runs the installer.			
jahlikes-- openssl_encrypt	openssl_encrypt versions before 1.4.9 contain a signature verification vulnerability in <code>gpg_runner.verify_detached</code> that accepts revoked and expired keys by only checking <code>VALIDSIG</code> status without inspecting <code>REVKEYSIG</code> , <code>EXPKEYSIG</code> , or <code>gpg</code> exit codes. Attackers holding compromised-then-revoked signing keys or expired project keys can bypass signature verification to execute malicious plugins in the host process.	2026-08-27	9.8	CVE-2026-81700
jahlikes-- openssl_encrypt	openssl_encrypt versions before 1.4.9 use a denylist to identify trusted built-in plugins, allowing unsigned plugins in top-level plugins/ directories and unknown subdirectories to bypass signature verification. Attackers can place malicious unsigned plugins following documented installation paths to achieve arbitrary code execution in the CLI process with access to passwords and cryptographic keys.	2026-08-27	9.8	CVE-2026-81701
jahlikes-- openssl_encrypt	openssl_encrypt before 1.4.9 fails to re-derive and validate fingerprints when loading identities from <code>identity.json</code> , allowing attackers to substitute public keys in identity stores. Attackers can replace legitimate public keys with their own while maintaining the claimed fingerprint, enabling silent key substitution where encryption uses attacker keys and signature verification appears valid.	2026-08-27	9.8	CVE-2026-81702
jahlikes-- openssl_encrypt	openssl_encrypt before 1.4.9 fails to sanitize the email field of imported identity documents, allowing attackers to inject ANSI escape sequences that forge the fingerprint verification line displayed to users. Attackers can deliver a crafted identity bundle through normal contact-exchange flows or keyserver responses to manipulate terminal output and display a fraudulent fingerprint, bypassing the out-of-band verification mechanism that protects against key substitution attacks.	2026-08-27	9.8	CVE-2026-81707
jahlikes-- openssl_encrypt	openssl_encrypt (pip package openssl-encrypt) versions 1.4.8 and earlier store an mTLS client private key in cleartext within a world-readable (0644) <code>SharedPreferences</code> file via the desktop GUI's Settings screen 'combined certificate and private key' PEM field. A local attacker with file system access can read the exposed private key. Version 1.4.9 writes the PEM to a dedicated 0600 file, keeps only its path in <code>SharedPreferences</code> , and migrates/scrubs existing cleartext values.	2026-08-27	8.4	CVE-2026-81683
jahlikes-- openssl_encrypt	openssl_encrypt versions before 1.4.9 store an unkeyed SHA-256 hash of the plaintext in the cleartext file header metadata. Attackers can read this hash without the password to confirm guessed plaintexts offline or fingerprint identical plaintexts across separately-encrypted files.	2026-08-27	7.5	CVE-2026-81688
jahlikes-- openssl_encrypt	openssl_encrypt versions before 1.4.9 derive the remote-pepper wrap key using unsalted HKDF-SHA256 or bare SHA-256 of the password, allowing identical keys across all users and files. Attackers with access to wrapped pepper blobs can precompute a single dictionary table and perform fleet-wide offline password guessing at hardware speed to recover user passwords.	2026-08-27	7.5	CVE-2026-81689
jahlikes-- openssl_encrypt	openssl-encrypt (pip package) before 1.4.9 contains a symlink-following flaw in its <code>verify-usb v2</code> added-file allowlist scan. The scan enumerated the drive with <code>rglob()</code> , which in CPython does not descend into symlinked directories and treats the symlink as an ordinary directory, while <code>O_NOFOLLOW</code> on the hash side binds only the final path component. An evil-maid attacker with physical access to the removable drive could replace a tool-tree directory with a symlink to a copy containing byte-identical files plus a planted <code>__pycache__/*.pyc</code> file (which CPython loads in preference to recompiling the clean <code>.py</code>). The planted file is never enumerated, <code>added_files</code> stays 0, and <code>verify-usb</code> reports <code>PASSED</code> , resulting in code execution when the victim runs the portable install. Fixed in 1.4.9 (affects both 1.4.x and 1.5.x lines).	2026-08-27	7.3	CVE-2026-81690
jahlikes-- openssl_encrypt	openssl_encrypt versions before 1.4.9 fail to validate server URLs in login and <code>register_with_email</code> functions, accepting unencrypted <code>http://</code> URLs and unconfigured hosts. Attackers on the network path can intercept cleartext credentials including <code>client_id</code> , passwords, and JWTs to achieve full keyserver account takeover.	2026-08-27	7.5	CVE-2026-81691
jahlikes-- openssl_encrypt	openssl_encrypt (pip: openssl-encrypt) versions 1.4.8 and earlier fail to validate the 36-bit <code>STREAMINFO total_samples</code> field of FLAC files before using it to size an allocation (<code>np.random.randint(size=(total_samples, channels))</code>). A ~50-byte crafted FLAC file declaring ~100 million samples causes a multi-gigabyte memory allocation, leading to out-of-memory denial of service during <code>'decrypt --stego-extract'</code> . The issue is fixed in 1.4.9; both the 1.4.x and 1.5.x lines are affected.	2026-08-27	7.5	CVE-2026-81692
jahlikes-- openssl_encrypt	openssl_encrypt before 1.4.9 fails to validate the total field from QR JSON payloads before materializing ranges. Attackers can supply crafted QR images with	2026-08-27	7.5	CVE-2026-81693

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	extremely large total values to trigger unbounded memory allocation and cause denial of service through out-of-memory conditions.			
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.9 contain a shell injection vulnerability in the info command's reconstructed CLI block that interpolates untrusted metadata fields without quoting. Attackers can craft metadata values like pepper_name containing shell commands that execute when users copy the printed CLI block into a shell.	2026-08-27	7.5	CVE-2026-81698
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.9 fail to properly validate key derivation function costs in crafted files, allowing attackers to trigger unbounded memory and CPU exhaustion during pre-authentication processing. Attackers can supply malicious files with excessive KDF parameters to exhaust system resources and crash or wedge the process before password verification occurs.	2026-08-27	7.5	CVE-2026-81699
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.9 contain a weak key derivation vulnerability in the D-Bus CryptoService.EncryptFile handler that uses unstretched SHA-256 instead of Argon2id. Attackers can perform offline password guessing against encrypted files roughly six to seven orders of magnitude faster than documented protection by exploiting the missing key stretching and hash rounds.	2026-08-27	7.5	CVE-2026-81704
jahlikes--openssl_encrypt	openssl-encrypt before 1.4.9 fails to redact the file password in its --debug argv dump when the password is supplied via bundled short-option spellings (e.g. -apHunter2) or abbreviated long-option spellings (e.g. --passw). The sanitizer only recognized exact option names, --option=value forms, and tokens starting with -p, so these spellings bypass the redaction chokepoint and the cleartext password is written to stderr. Anyone with access to that output (terminal scrollback, merged 2>&1 output, CI job logs, or the GUI's persistent debug log) can recover the password.	2026-08-27	7.5	CVE-2026-81705
jahlikes--openssl_encrypt	openssl_encrypt (pip: openssl-encrypt) versions <= 1.4.8 use suffix-tolerant fingerprint matching in enroll_trust_key when binding a plugin-signing trust anchor. An operator who confirms a short (forgeable, ~32-bit) GPG key id could unknowingly enroll an attacker's colliding key as a trusted anchor, which then vouches for malicious plugins under the ENFORCE signature policy. Version 1.4.9 fixes this by requiring the confirmed value to exactly match the full primary-key fingerprint (case-insensitive, whitespace-stripped).	2026-08-27	7	CVE-2026-81714
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.9 use under-parameterized PBKDF2-HMAC-SHA256 with only 100,000 iterations to protect PQC keyfile private keys and 10,000 iterations for dual-encryption file-password verification. Attackers who obtain keyfiles or encrypted files can brute-force wrapping passwords offline using GPU or ASIC acceleration.	2026-08-27	7.5	CVE-2026-81718
jahlikes--openssl_encrypt	openssl_encrypt before 1.4.9 executes untrusted third-party plugins with insufficient controls: the plugin signature policy defaulted to WARN, so an unsigned/unverifiable non-built-in plugin was compiled and executed in the host process at import time, before the runtime sandbox is installed. The only default gate was an incomplete, bypassable AST denylist. If a user is induced to load an attacker's plugin, this results in arbitrary code execution with the privileges of the user running openssl_encrypt. Fixed in 1.4.9 by defaulting the signature policy to ENFORCE for non-built-in plugins.	2026-08-27	7.8	CVE-2026-81719
jahlikes--openssl_encrypt	openssl_encrypt before 1.4.9 fails to validate KDF cost parameters in encrypted file metadata and keystore headers, allowing attackers to trigger unbounded memory allocation. Attackers can craft malicious encrypted files declaring arbitrarily large Argon2, scrypt, or balloon KDF parameters to exhaust system memory and crash the process without authentication.	2026-08-27	7.5	CVE-2026-81721
jeremyevans--rodauth	Rodauth before 2.46.0 contains an authentication bypass vulnerability in the webauthn_login route that allows logged-in users to authenticate as any other account. Attackers can exploit improper account resolution logic that falls back to session account identifiers instead of validating the credential binding to complete authentication as arbitrary users.	2026-08-29	8.7	CVE-2026-82466
jfrog--artifactory	JFrog Artifactory contains an authentication weakness that, under default configuration, may allow an unauthenticated attacker with network access to obtain administrative privileges.	2026-08-28	9.8	CVE-2026-82329
jfrog--artifactory	A user who can read an existing remote VCS repository can replace its configured origin or supply an absolute VCS data URL.	2026-08-25	8.5	CVE-2026-70551
jfrog--artifactory	An authenticated user may initiate repository migration operations without required repository permissions, potentially causing information disclosure, unauthorized state changes, and service disruption. Fixed versions address the issue.	2026-08-25	7.6	CVE-2026-69104

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jina-ai--reader	jina-ai reader disables its private-address guard outside Google Cloud deployments, allowing unauthenticated attackers to perform server-side request forgery. Attackers can supply publicly resolvable hostnames mapping to private addresses to retrieve cloud metadata and internal service content.	2026-08-30	7.5	CVE-2026-82638
Jonathan de Jong--Beautiful Taxonomy Filters	Unauthenticated SQL Injection in Beautiful Taxonomy Filters <= 2.4.6 versions.	2026-08-27	9.3	CVE-2026-78288
jQWidgets--jQWidgets	A vulnerability was determined in jQWidgets up to 24.0.1. This affects the function JQXLite.extend/jqxBaseFramework.extend of the file jqwidgets/jqx-all.js. This manipulation causes improperly controlled modification of object prototype attributes. The attack can be initiated remotely. The reported GitHub issue was closed with the label "not planned".	2026-08-24	7.3	CVE-2026-78178
Kalles Addons--Kalles Addons	The Kalles Addons plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.6 via deserialization of untrusted input. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present.	2026-08-25	8.1	CVE-2026-78572
kazuph--mcp-fetch	mcp-fetch checks a fetch target against its SSRF guard without removing the brackets that surround an IPv6 literal. isSafeUrl reads the hostname from the parsed URL, which for a literal such as http://[::1]/ yields the bracketed string, and then tests it with net.isIP. That call returns zero for a bracketed value, so the branch holding the private-address checks is skipped entirely. The guard falls back to resolving the hostname, the bracketed string is not a resolvable name, no addresses are returned, and the target is reported safe. The HTTP client then strips the brackets and connects. Because the address may be given in IPv4-mapped form, the same path reaches any IPv4 target the loopback and private checks were meant to exclude, including link-local metadata endpoints. isPrivateIPv6 also has no case for the ::ffff: prefix, so the mapped form would still pass even if the brackets were removed. The fetch target is supplied as a tool argument, so an attacker who can influence what the model requests can read internal responses back into the model context.	2026-08-26	7.5	CVE-2026-80347
keploy--keploy	keploy versions 3.1.0 through 3.6.25 bind the agent control-plane HTTP server to all interfaces without authentication, exposing endpoints that stream TLS session keys and traffic data. Attackers can access the /agent/pcap/keylog endpoint to retrieve NSS keylog lines and decrypt recorded TLS traffic, or invoke /agent/stop and /agent/storemocks to manipulate recording sessions.	2026-08-30	8.6	CVE-2026-82641
kimai--kimai	Kimai before 2.62.0 fails to validate create_other_timesheet permission in the QuickEntry controller when creating new timesheets. Authenticated users with view_other_timesheet and edit_other_timesheet permissions can create timesheet records for team members by submitting the QuickEntry form, bypassing authorization checks enforced elsewhere.	2026-08-25	8.8	CVE-2026-80193
kimai--kimai	Kimai before 2.56.0 does not enforce team-membership checks in TimesheetVoter::voteOnAttribute(), which maps permissions only to own_timesheet or other_timesheet. As a result, any authenticated user with ROLE_TEAMLEAD (or a role holding edit_other_timesheet/delete_other_timesheet) can read, modify, and permanently delete timesheets belonging to any user system-wide via the API, regardless of team membership. Timesheet IDs are sequential integers and trivially enumerable. ROLE_USER accounts are correctly restricted. (Note: the maintainers characterize this behavior as matching the documented permission model.)	2026-08-25	8.8	CVE-2026-80202
kimai--kimai	Kimai before 2.58.0 contains an authentication bypass vulnerability where password reset links remain valid after password changes because the LoginLink signature covers only the user id, not the password hash. Attackers who intercept or cache a password reset link can use it up to 2 additional times within a 1-hour window to log in as the user even after the legitimate user has changed their password.	2026-08-25	7.5	CVE-2026-80196
kimai--kimai	Kimai versions before 2.56.0 fail to restrict the config() Twig function in sandboxed invoice and export templates, allowing administrators to access arbitrary configuration keys. Attackers with admin privileges can upload malicious templates to exfiltrate server-wide secrets including LDAP bind passwords and SAML private keys into invoice or export documents accessible to lower-privileged users.	2026-08-25	7.5	CVE-2026-80198

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kitae-park--Mang Board WP	The Mang Board WP plugin for WordPress is vulnerable to Missing Authorization via Authentication Cookie Forgery in all versions up to, and including, 2.3.7. This is due to flawed HMAC generation in the mbw_get_hash_key() function that uses the current user's identity instead of the cookie username parameter when a WordPress user is logged in, combined with insufficient validation in mbw_validate_auth_cookie(). This makes it possible for authenticated attackers, with subscriber-level access and above, to forge administrator authentication cookies and change administrator passwords to achieve complete site takeover.	2026-08-26	8.8	CVE-2026-75977
KlbTheme--Total Donations	The Total Donations plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 2.0.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-25	9.8	CVE-2026-78568
KlbTheme--Total Donations	The Total Donations plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 2.0.5. This makes it possible for unauthenticated attackers to elevate their privileges to that of an adminstrator.	2026-08-25	9.8	CVE-2026-78570
klever-io--klever-go	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.19, marketplace settlement in core/kapp/market/market.go reads MarketOrderData.ReferralPercentage from the listing while reading asset.Royalties.MarketPercentage live at purchase time. An asset owner can create a valid listing and then use AssetTrigger UpdateRoyalties to make the combined referral and royalty percentages exceed the bid. executeBuyMarket pays referral and royalty amounts unconditionally while computeMarketOwnerAmount silently skips a nonpositive seller remainder, allowing MarketBuy, BuyItNow, or auction Claim settlement to credit more KLV or sale currency than the buyer paid. This can create unbacked currency and corrupt token supply integrity. This issue is fixed in version 1.7.19.	2026-08-28	9.6	CVE-2026-54754
klever-io--klever-go	Klever-Go is the Go implementation of the Klever blockchain protocol. Prior to 1.7.19, split-royalty fields decoded in core/kapp/builtinFunctions/utlis.go can contain values greater than core.HundredPercent, and core/kapp/kda/create.go and core/kapp/kda/trigger.go sum those values in uint32 accumulators. Crafted values such as two 0x80000000 entries wrap the validation sum to zero and pass CheckValid100Params. Royalty payout paths in core/kapp/accounts/accounts.go, core/kapp/market/market.go, and core/kapp/ito/ito.go then credit each oversized split amount and silently discard a negative remainder, allowing ordinary asset transfers, marketplace purchases, or ITO purchases to create unbacked KLV or other assets. This issue is fixed in version 1.7.19.	2026-08-28	9.6	CVE-2026-54755
kubeedge--kubeedge	KubeEdge CloudCore through 1.23.1 accepts node task status reports on its HTTPS server without authentication verification. Attackers can reach CloudCore on port 10002 to mark upgrade jobs as succeeded or failed, deceiving the control plane about node upgrade status and blocking further upgrade scheduling.	2026-08-29	8.2	CVE-2026-82473
kubeflow--pipelines	Kubeflow Pipelines enables users to build and deploy portable, scalable machine learning workflows. Prior to 2.17.0, the Kubeflow Pipelines frontend exposes an unauthenticated server-side request forgery vulnerability through the /_proxy/ route in frontend/server/proxy-middleware.ts. The _routePathWithReferer() function accepts an arbitrary attacker-controlled HTTP or HTTPS target and passes its origin to createProxyMiddleware without a host allowlist or filtering for loopback, link-local, RFC1918, or cluster-local addresses. The route remains outside the authorization middleware when ENABLE_AUTHZ=true and is reachable through /apis/v1beta1/_proxy/, /apis/v2beta1/_proxy/, /pipeline/apis/v1beta1/_proxy/, and /pipeline/apis/v2beta1/_proxy/, including through a crafted Referer header. Requests can forward attacker-controlled methods, headers such as Authorization, Cookie, and X-Forwarded-For, and POST bodies to reachable internal services, while returning the upstream response to the unauthenticated client. This can expose cloud metadata credentials, Kubernetes or service APIs, and other cluster-internal endpoints to unauthorized read or modification. This issue is fixed in version 2.17.0.	2026-08-28	10	CVE-2026-54745
kubevela--kubevela	KubeVela is an open source application delivery platform. Prior to 1.9.14, from 1.10.0-alpha.1 until 1.10.9, and from 1.11.0-alpha.1 until 1.11.0-alpha.4, the Terraform remote configuration loader in pkg/controller/utlis/capability.go, GetTerraformConfigurationFromRemote, clones a repository supplied through a core.oam.dev/v1beta1 ComponentDefinition and follows repository-controlled variables.tf or main.tf symlinks. A user with permission to create or update	2026-08-28	8.5	CVE-2026-55108

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ComponentDefinition objects can point variables.tf to /dev/zero through terraform.path, after which os.Stat and os.ReadFile follow the link and read an unbounded stream before ParseTerraformVariables or HCL parsing can reject the content. The read can exhaust memory, OOM-kill the cluster-wide vela-core controller, cause repeated Pod restarts, and pressure node memory when no effective container limit is configured. This issue is fixed in versions 1.9.14, 1.10.9, and 1.11.0-alpha.4.			
kyverno--kyverno	Kyverno is a policy engine designed for cloud native platform engineering teams. From 1.18.0 until 1.18.2, the NamespacedMutatingPolicy CEL compiler exposes the generator library to matchConditions, allowing a namespace-scoped policy to invoke generator.apply(namespace, resources) with an arbitrary target namespace. The validation in pkg/cel/policies/mpol/validate.go checks that the policy compiles but does not enforce namespace scope, and GenerateResources in pkg/cel/libs/context.go does not reject the cross-namespace target. A user who can create NamespacedMutatingPolicy objects in one namespace can cause the admission controller, operating with cluster-wide privileges, to create ConfigMaps, NetworkPolicies, Secrets, RoleBindings, and other resources in another namespace, enabling unauthorized modification and potential privilege escalation. This issue is fixed in version 1.18.2.	2026-08-26	9.6	CVE-2026-54523
Le-yan--Medical Practice Management System	Medical Practice Management System developed by Le-yan has a Remote Code Execution vulnerability. Unauthenticated remote attackers can execute arbitrary OS commamnds via a crafted HTML page.	2026-08-25	8.8	CVE-2026-78685
Lektor--Lektor	A path traversal vulnerability exists in the built-in preview/development web server of Lektor <3.3.14 on Windows. An attacker with network access to the server can send a crafted HTTP request containing path traversal sequences to read arbitrary files accessible to the process, disclosing sensitive information such as system files and deployment configuration files containing credentials.	2026-08-27	7.5	CVE-2026-75418
lepture--mistune	Mistune is a Python Markdown parser with renderers and plugins. Versions 3.3.0 through 3.3.2 are vulnerable to DoS through deeply nested tokens. HTML rendering creates deeply nested emphasis tokens from consecutive asterisk characters, and recursive rendering in HTMLRenderer.render_token() can exceed Python's recursion limit and raise RecursionError, allowing crafted Markdown to crash a parsing process. This issue is fixed in version 3.3.3	2026-08-24	7.5	CVE-2026-76098
libp2p--js-libp2p	libp2p is a JavaScript implementation of the libp2p networking stack. Prior to version 4.2.9, the reservation refresh path in reservation-store.ts reuses the same retimeableSignal but unconditionally registers another abort listener on every refresh. As a result, a remote peer can repeatedly send valid RESERVE requests for the same reservation, causing unbounded listener and closure growth in @libp2p/circuit-relay-v2 relay servers and leading to denial of service. This issue is fixed in version 4.2.9.	2026-08-24	7.5	CVE-2026-77384
LikeBtn--Like Button Rating	Subscriber SQL Injection in Like Button Rating <= 2.6.61 versions.	2026-08-27	8.5	CVE-2026-78285
limanmys--core	Liman is open source server management software. Prior to 2.2.2 - 1103, an OS command injection vulnerability in the log rotation configuration endpoint allows an authenticated administrator to execute arbitrary operating system commands on the Liman server. The 'ip_address' parameter is embedded directly into a shell command without sanitization, enabling shell escape via single-quote injection. This is fixed in 2.2.2 - 1103.	2026-08-27	9.1	CVE-2026-57499
lin-snow--Ech0	Ech0 through 4.5.6 contains an OAuth redirect URI validation vulnerability in parseAndValidateClientRedirect (internal/service/auth/auth.go) that compares only the scheme and host of the client-supplied redirect_uri against the admin-configured allowlist, ignoring path, query, and fragment components. The redirect_uri is embedded into the signed state JWT at login time without validation. An attacker can craft a redirect_uri whose host matches an allowed origin but whose path is attacker-influenced; after the OAuth exchange the victim is redirected to that path with a one-time exchange code in the query string. If the code leaks (e.g., via Referer, analytics, or an open redirect on that host), the attacker can trade it at the public POST /api/auth/exchange endpoint for the victim's access and refresh tokens. Fixed in 4.7.3.	2026-08-25	8	CVE-2026-79662
lin-snow--Ech0	Ech0 before 4.5.1 contains an authorization bypass vulnerability where session tokens skip scope validation in RequireScopes middleware, allowing logged-in non-admin users to access admin endpoints. Attackers can read system logs, visitor	2026-08-25	8.8	CVE-2026-79665

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	statistics, user emails, and subscribe to live WebSocket logs by sending authenticated session tokens to unprotected endpoints.			
lin-snow--Ech0	Ech0 before 5.0.1 does not impose any size or shape limit on the Accept-Language header processed by its i18n middleware, which runs on every HTTP request. The header is passed unfiltered to go-i18n's NewLocalizer, which internally calls <code>golang.org/x/text/language.ParseAcceptLanguage</code> . The CVE-2022-32149 mitigation in <code>x/text</code> caps '-' characters but not '_' characters, which the parser aliases to '-', allowing quadratic-time parsing to be triggered with a large header (up to Go's default 1 MiB) built from underscore separators. An unauthenticated attacker can send such requests to consume roughly 1.5 seconds of CPU each, and concurrent requests can saturate a multi-core server (denial of service).	2026-08-25	7.5	CVE-2026-79658
lin-snow--Ech0	Ech0 before 4.7.3 contains a server-side request forgery vulnerability in the <code>fetchPeerConnectInfo</code> function that uses unvalidated HTTP requests instead of safe request methods with URL validation. Authenticated attackers can supply arbitrary URLs to access internal services and cloud metadata endpoints by triggering connection health checks or peer connection operations.	2026-08-25	7.7	CVE-2026-79659
lin-snow--Ech0	Ech0 before 4.7.3 fails to properly revoke access tokens created with never-expire option, allowing attackers to maintain perpetual authenticated access after token theft. Three independent revocation mechanisms fail: logout panics on nil <code>ExpiresAt</code> field, <code>RevokeToken</code> skips when <code>remainTTL</code> is zero, and admin delete does not blacklist the JTI, leaving stolen tokens cryptographically valid until JWT secret rotation.	2026-08-25	7.4	CVE-2026-79664
lin-snow--Ech0	Ech0 version 4.3.4 and earlier fails to reliably enforce scoped access token (least-privilege) restrictions on several privileged admin routes. Multiple privileged endpoints (e.g., <code>/api/inbox</code> , <code>/api/panel/comments</code> , <code>/api/backup/export</code>) omit scope checks and authorize based only on the user's admin role, and the backup export handler discards token scope metadata entirely. An attacker holding a deliberately limited (low-scope) admin access token can reach broader privileged functionality than intended, including reading the inbox and exporting a full database backup ZIP archive. Fixed in 4.4.3.	2026-08-25	7.6	CVE-2026-79667
Linux Foundation--Magma	A vulnerability was identified in Linux Foundation Magma 1.9.0. This affects an unknown function of the component <code>SecurityModeComplete</code> Handler. Such manipulation leads to improper validation of integrity check value. The attack may be launched remotely. The exploit is publicly available and might be used.	2026-08-30	8.3	CVE-2026-82549
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>net: ethernet: ti: am65-cpsw-nuss: Fix port_id extraction from SRC TAG</code> On the packet reception path, the ID of the MAC Port on which the packet was received, is embedded in the RX DMA Descriptor's metadata. The ID is extracted using the helper function <code>cppi5_desc_get_tags_ids()</code> which fills in the 16-bit Source Tag into the 'port_id' variable. However, it is only the lower 8-bits of the 16-bit Source Tag that represent the MAC Port ID, while the upper 8-bits are Hardware-Reserved and carry an arbitrary value. With the existing logic, sporadic kernel crash is observed due to the subsequent driver code accessing out-of-bound memory because of an invalid <code>port_id</code> . Hence, fix the <code>port_id</code> extraction logic to use only the lower 8-bits of the Source Tag as the MAC Port ID.	2026-08-26	9.8	CVE-2026-74737
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>macvlan: inherit needed_headroom and needed_tailroom from lowerdev</code> macvlan devices inherit <code>hard_header_len</code> from lowerdev during <code>macvlan_init()</code> , but leave <code>needed_headroom</code> and <code>needed_tailroom</code> set to 0. When the underlying lowerdev requires extra headroom or tailroom for headers/trailers (e.g. <code>macsec</code> , <code>ipsec</code> , <code>wireguard</code> , <code>tunnels</code> , or <code>veth</code> with rx headroom), upper layers calculating packet headroom and tailroom fail to reserve sufficient space. This can result in reallocation overhead, <code>skb</code> headroom underflows, or KASAN slab-use-after-free crashes when <code>dev_hard_header()</code> / <code>macvlan_hard_header()</code> prepends header data or when lower devices append tailroom. Fix this by: 1. Inheriting <code>needed_headroom</code> and <code>needed_tailroom</code> from lowerdev in <code>macvlan_init()</code> . 2. Propagating <code>needed_headroom</code> and <code>needed_tailroom</code> updates to attached macvlans in <code>macvlan_device_event()</code> when receiving <code>NETDEV_FEAT_CHANGE</code> events.	2026-08-26	9.8	CVE-2026-74743
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>ipvlan: inherit needed_headroom and needed_tailroom from phy_dev</code> <code>ipvlan</code> devices inherit <code>hard_header_len</code> from <code>phy_dev</code> during <code>ipvlan_init()</code> , but leave <code>needed_headroom</code> and <code>needed_tailroom</code> set to 0. When the underlying <code>phy_dev</code> (or stacked lower device) requires extra headroom or tailroom for headers/trailers (e.g. <code>macsec</code> ,	2026-08-26	9.8	CVE-2026-74744

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ipsec, wireguard, tunnels, or veth with rx headroom), upper layers calculating packet headroom and tailroom fail to reserve sufficient space. This can result in reallocation overhead, skb headroom underflows, or KASAN slab-use-after-free crashes when dev_hard_header() / ipvlan_hard_header() prepends header data or when lower devices append tailroom. Fix this by: 1. Inheriting needed_headroom and needed_tailroom from phy_dev in ipvlan_init(). 2. Propagating needed_headroom and needed_tailroom updates to attached ipvlans in ipvlan_device_event() when receiving NETDEV_FEAT_CHANGE events.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: publish GC-visible tuple last nf_flow_table_iterate() only treats original-direction tuple nodes as owning entries. Publishing the original node first lets GC observe and free a flow while flow_offload_add() is still inserting the reply node. Publish the reply node first and the original node last so GC never sees a partially installed flow. KASAN can trigger slab-use-after-free read and write reports in the flowtable/rhashtable path (rht_deferred_worker, jhash, flow_offload_del, flow_offload_lookup, etc.).	2026-08-26	9.8	CVE-2026-74746
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: riscv: lib: Fix ZBB strnlen reading past count boundary The ZBB-optimized strnlen loop loads one word ahead before checking the aligned boundary: REG_L t1, SZREG(t0) // load next word addi t0, t0, SZREG // advance orc.b t1, t1 bgeu t0, t4, 4f // boundary check AFTER load where t4 = (s + count) & -SZREG. When s is aligned and count is a multiple of SZREG, t4 equals s + count and the loop loads a full word starting at exactly s + count. If s + count falls on a page boundary with the next page unmapped, this faults. Fix by computing the aligned boundary from the last valid byte (s + count - 1) instead of s + count. This makes the loop stop at the word containing the last valid byte rather than potentially loading the word after it. The count == 0 case is already handled by the beqz early exit. Also add a pre-loop guard (bgeu t0, t4) for the case where all valid bytes fit within the first word. With the adjusted boundary, t4 can equal t0, and entering the loop with stale register state from the first-word processing would produce incorrect results. The final minu clamp ensures the result is still correct when the last loaded word extends past s + count - 1 within the same aligned word.	2026-08-26	9.4	CVE-2026-74751
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: validate cookie AUTH state before use When cookie authentication is disabled, COOKIE_ECHO restores fixed-size AUTH fields directly from peer-controlled cookie bytes. A forged RANDOM length, HMAC list, or CHUNKS list can then reach association consumers with lengths or identifiers that were never validated against the local backing arrays. A forged RANDOM length can cause out-of-bounds reads during key-vector construction. A forged HMAC identifier also caused a 32-byte write past a zero-length AUTH chunk, providing a primitive for a local privilege escalation chain. Validate the cookie's RANDOM, HMACS, and CHUNKS parameters at the cookie trust boundary before copying them into the association. Reject invalid types, malformed lengths, unsupported HMAC identifiers, HMAC lists without SHA1, and forbidden chunk ids.	2026-08-26	9.8	CVE-2026-74752
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ovpn: finish crypto callback cleanup before peer release Crypto completion callbacks hold both key-slot and peer references. The peer reference pins the netdev, and dropping the last peer reference can let netdev unregistration and module removal make progress. Do not release that peer reference before the callback has finished its own cleanup. If ovpn_crypto_key_slot_put runs after ovpn_peer_put, it can schedule an RCU callback backed by module text after ovpn_cleanup_rcu_barrier has already run. The TX error path also freed the remaining skb after ovpn_peer_put, leaving callback cleanup outside the peer/netdev lifetime window. Release the key slot and free any remaining skb first, then drop the peer reference as the last callback action.	2026-08-26	9.8	CVE-2026-80519
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ceph: avoid fs reclaim while using current->journal_info handle_reply() stores a `ceph_mds_request` pointer in `current->journal_info` while filling the inode and dentry cache from an MDS reply. An allocation in this section can enter direct reclaim and prune dentries from another filesystem. If this dirties an ext4 inode, ext4 starts a JBD2 transaction. JBD2 interprets the Ceph request in `current->journal_info` as a journal handle and dereferences the request's `r_tid` as `h_transaction`, causing a kernel crash, e.g.: Unable to handle kernel paging request at virtual address 00000000077b4818 [...] Internal error: Oops: 0000000096000004 [#1] SMP Modules linked in: CPU: 6 UID: 0 PID: 2699135	2026-08-26	9.8	CVE-2026-80528

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Comm: kworker/6:3 Tainted: G W 6.18.38-i3 #1113 NONE [...] Workqueue: ceph-msgr ceph_con_workfn pstate: 80400009 (Nzcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : jbd2__journal_start+0x2c/0x208 lr : __ext4_journal_start_sb+0x100/0x178 [...] Call trace: jbd2__journal_start+0x2c/0x208 (P) __ext4_journal_start_sb+0x100/0x178 ext4_dirty_inode+0x3c/0x90 __mark_inode_dirty+0x58/0x400 iput.part.0+0x2b0/0x370 iput+0x18/0x30 dentry_unlink_inode+0xc0/0x158 __dentry_kill+0x80/0x250 shrink_dentry_list+0x90/0x130 prune_dcache_sb+0x60/0x98 super_cache_scan+0xe8/0x190 do_shrink_slab+0x174/0x388 shrink_slab+0xd8/0x4c0 shrink_node+0x31c/0x908 do_try_to_free_pages+0xd0/0x508 try_to_free_pages+0x11c/0x238 __alloc_frozen_pages_noprof+0x4d0/0xdd0 __folio_alloc_noprof+0x18/0x70 __filemap_get_folio+0x248/0x440 ceph_readdir_prepopulate+0x570/0x9e8 mds_dispatch+0x1424/0x1ba0 ceph_con_process_message+0x74/0xa0 ceph_con_v1_try_read+0x3a0/0x1510 ceph_con_workfn+0x260/0x460 Enter a scoped NOFS allocation context and leave it after clearing `journal_info`. This prevents filesystem reclaim from recursing into another filesystem while the field contains Ceph-private data.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Ensure first IDAW remains constant The first IDAW in a list does not need to be on a 2K/4K boundary like all others, and so is read separately to accurately calculate the size of the buffer needed to read the full IDAL. Verify that the address found in the first IDAW is unchanged between reads, to ensure a consistent set of IDAWs being worked with.	2026-08-26	9.3	CVE-2026-80551
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Limit the number of channel program segments The processing of channel programs, and the CCWs within them, is done recursively. As such, there is an arbitrary (but not architectural) limit to the number of CCWs that can exist in a single channel program. The vfio-ccw logic breaks these channel programs into segments whenever it encounters a Transfer-In-Channel (TIC) CCW, and the combined number of segments count towards the global limit. Impose an equivalent limit to the number of segments until such logic can be made non-recursive.	2026-08-26	9.3	CVE-2026-80554
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: fix OOB read in decode_watchers() via missing bounds check ceph_start_decoding() validates that struct_len bytes remain in the buffer after the encoding header, but accepts struct_len=0 as valid: ceph_decode_need(p, end, 0, bad) always passes. When a malicious or compromised OSD sends an obj_list_watch_response_t reply with struct_len=0, ceph_start_decoding() returns success with p == end, leaving zero bytes guaranteed for subsequent reads. The immediately following ceph_decode_32(p) in decode_watchers() has no preceding bounds check. With p == end this is a 4-byte read past the validated buffer boundary. The garbage value is then passed directly to kzalloc_objs() as the watcher count. The sibling function decode_watcher() already uses the safe variants (ceph_decode_copy_safe, ceph_decode_64_safe, ceph_decode_skip_32) after its own ceph_start_decoding() call. decode_watchers() is the only site that uses the bare variant, confirming an oversight. Fix by replacing ceph_decode_32(p) with ceph_decode_32_safe(p, end, *num_watchers, bad), consistent with the established pattern. Attacker model: a malicious or compromised OSD in a multi-tenant Ceph deployment (e.g. cloud) can trigger this against any kernel client that calls CEPH_OSD_OP_LIST_WATCHERS, without any further privileges beyond OSD session establishment. [idryomov: trim changelog]	2026-08-26	9.8	CVE-2026-80557
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: Avoid using invalid osd indices from primary_temp A corrupted osdmap received from a Ceph monitor or OSD may contain osd indices in its pg_temp, primary_temp, pg_upmap, and pg_upmap_items parts that don't exist, i.e., that are greater than max_osd or smaller than CEPH_HOMELESS_OSD (-1). These indices are used to create the up and acting set in ceph_pg_to_up_acting_osds(), called from calc_target(). While most of these osd indices are checked, the one from primary_temp is not. Subsequently, this may lead to calc_target() returning this (potentially invalid) index as target osd for a (linger) request. Because the osd_state, osd_weight, and osd_addr arrays only contain max_osd entries (with indices 0 to max_osd - 1), this leads to out-of-bounds accesses when trying to read values from these arrays. This patch fixes the issue by adding a check to get_temp_osds(), so that only valid osd indices from primary_temp are used, and it	2026-08-26	9.8	CVE-2026-80558

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	falls back to using the primary from pg_temp or the up set if it is invalid. [idryomov: changelog]			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: fix multiple unsafe decodes in decode_locker() decode_locker() in cls_lock_client.c contains three unsafe decode operations that allow a malicious or compromised OSD to trigger slab-out-of-bounds reads: 1. ceph_decode_copy() at the locker_id_t name field has no preceding bounds check. With p == end after ceph_start_decoding() accepts struct_len=0, this reads sizeof(ceph_entity_name) = 9 bytes past the validated buffer boundary. 2. *p += sizeof(struct ceph_timespec) after the locker_info_t header is an unchecked pointer advance. A malicious OSD can position p past end, causing all subsequent _safe checks to pass against a bogus boundary. 3. len = ceph_decode_32(p) has no preceding bounds check, and the immediately following *p += len is uncapped. A malicious OSD can send len=0xffffffff, advancing p gigabytes past end and escaping the decode window entirely. Fix all three by replacing bare operations with their safe variants: ceph_decode_copy -> ceph_decode_copy_safe *p += sizeof(...) -> ceph_decode_skip_n ceph_decode_32(p) -> ceph_decode_32_safe *p += len -> ceph_decode_skip_n A new label is added to return -EINVAL on any bounds violation. -EINVAL is appropriate here: the data received from the OSD is structurally malformed, which is an invalid argument to the decode contract regardless of whether the caller or the wire is at fault. Attacker model: a malicious or compromised OSD in a multi-tenant Ceph deployment can trigger this against any kernel client that issues the lock.get_info class method (e.g. during RBD exclusive lock acquisition) without any further privileges beyond OSD session establishment. [idryomov: use ceph_decode_skip_string() to skip description, trim changelog]	2026-08-26	9.8	CVE-2026-80561
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: fastopen: only mark MPTFO subflows with SYN data Passive TCP Fast Open accepts a valid-cookie SYN even when it carries no data. In that case the child socket's receive queue is intentionally left empty. mptcp_fastopen_subflow_synack_set_params() set is_mptfo before checking for queued SYN data. That made data-less TFO SYNs hit a WARN and, if the warning was non-fatal, left stale MPTFO state behind. The stale flag could later trigger a state-confusion bug in check_fully_established(). Only mark the subflow as MPTFO after confirming that an SKB was queued. Return quietly when the receive queue is empty. Note that mptcp_subflow_context's is_mptfo field is now not just about subflows where the TFO was present, but about MPTFO subflow that consumed SYN data. Only having a valid cookie but not carrying data is not really "doing TFO".	2026-08-26	9.4	CVE-2026-80585
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: options: reset DSS fields in case of unexpected size A remote peer could send a malformed DSS with a wrong size, followed by another DSS or MPC + Data. In this case, the first suboption will be ignored, but leaving some fields written, which could lead to inconsistency or access uninitialized data. Explicitly reset the fields that could have been modified in case of unexpected size.	2026-08-26	9.8	CVE-2026-80586
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: avoid combining some incoming suboptions Some MPTCP suboptions are mutually exclusive according to the RFC8684, but also because in different places, the code doesn't expect some combinations to be present. That's specially true for suboptions that would be present twice, but with different attributes. The new restrictions are the same as the ones applied on the output side, with mptcp_write_options. The same rules can be reused with a small fix: an MP_FASTCLOSE can be used with a DSS when the sender picks this option [1], which is not the case on Linux. Here are the rules: Which options can be used together? X: mutually exclusive O: often used together C: can be used together in some cases P: could be used together but we prefer not to (optimisations) Opt: MPC MPJ DSS ADD RM PRIO FAIL FC ----- ----- ----- ----- ----- ----- ----- ----- MPC ----- ----- ----- ----- ----- ----- ----- MPJ X ----- ----- ----- ----- ----- ----- DSS X X ----- ----- ----- ----- ----- ADD X X P ----- ----- ----- ----- RM C C C P ----- ----- PRIO X C C C C ----- ----- FAIL X X C X X X X ----- FC X X P X X X X ----- RST X X X X X X X O O ----- ----- ----- ----- ----- ----- ----- The only difference is with the 'P': another stack could send and ADD_ADDR with other suboptions (DSS, RM_ADDR), and this should be allowed. A few points of attention: - In theory, an MP_CAPABLE could be used with a RM_ADDR, but there is no reason to add it with	2026-08-26	9.8	CVE-2026-80587

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a SYN. Note that even with a 4th ACK, it doesn't seem to be useful, except when IDs are known in advance via another channel. Better not to break that. - Now, combining both an MP_CAPABLE and an MP_JOIN will no longer result to a reject of the two options, but only the second suboption is ignored. That seems OK to do that for this unexpected error. At least now all inconsistent combinations are handled the same way. This could change later in next. This also means the explicit checks for having both MPC + MPJ in subflow.c will now be unreachable. That's fine, they will be removed in a follow-up patch. - In case of conflicting combinations, the extra suboption(s) is/are ignored: having such combinations either means the remote peer is buggy, or is evil. The simplest action is then taken in this case: stop processing the current suboption. - In mp_opt->suboptions, there is also a bit reserved to the checksum, which can be used in an MP_CAPABLE and a DSS. Each time a DSS option can be used in parallel with another option, the checksum can be set, so the verification is combined into a new OPTIONS_MPTCP_DSS macro. - An MP_CAPABLE ACK can carry a Data-Level Length, and an optional Checksum: they are the same as the ones found in a DSS, because a DSS cannot be used in parallel to an MP_CAPABLE. Similarly, even if there is room, a DSS cannot be used with an MP_JOIN.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: block: stop the timeout timer when releasing a never added disk disk_release() undoes blk_mq_init_allocated_queue() for a disk whose probe failed before add_disk(), but it only calls blk_mq_exit_queue(). Nothing there stops q->timeout, and that timer rolls forward: it stays pending until it next expires, not until the last request completes. So if the driver issued any I/O before adding the disk, the request_queue is freed while still linked into a timer wheel bucket. Commit 6f8191fdf41d ("block: simplify disk shutdown") dropped the blk_cleanup_queue() call that used to stop it. __del_gendisk() and blk_mq_destroy_queue() still do; only the probe failure path lost it. nvme gets there because nvme_update_ns_info() submits Report Zones or FDP io-mgmt-recv on ns->queue before the disk is added, so a later failure - a concurrent reset setting NVME_CTRL_FROZEN, or device_add_disk() failing - lands in put_disk() with the timer armed: BUG: KASAN: slab-use-after-free in detach_if_pending+0x30c/0x340 Write of size 8 at addr ffff888004d71310 by task kworker/u8:2/37 __timer_delete_sync+0x156/0x240 kernel/time/timer.c:1621 blk_sync_queue+0x22/0x40 block/blk-core.c:222 nvme_sync_queues+0x100/0x150 drivers/nvme/host/core.c:5362 nvme_reset_work+0x138/0x930 drivers/nvme/host/pci.c:3264 Allocated by task 34: __blk_mq_alloc_disk+0x33/0x100 block/blk-mq.c:4462 nvme_alloc_ns+0x290/0x3870 drivers/nvme/host/core.c:4146 Freed by task 0: blk_free_queue_rcu+0x3a/0x50 block/blk-core.c:254 rcu_core+0xc10/0x1730 kernel/rcu/tree.c:2857 The queue being synced there is ctrl->admin_q, only a victim sharing a timer wheel bucket with the freed queue's dangling entry; other runs tripped in enqueue_timer(), __run_timers() or blk_mq_timeout_work(). Failing nvme_alloc_ns() with a debug patch makes it deterministic: one leaked timer trips KASAN within seconds, while 1987 patched releases produced no splat. Stop the timer and the queue work items before blk_mq_exit_queue(), like blk_mq_destroy_queue() does. Found by FuzzNvme.	2026-08-26	9.8	CVE-2026-80589
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: dat: acquire ARP hw source only after skb realloc The pskb_may_pull() called by batadv_get_vid() could reallocate the buffer behind the skb. Variables which were pointing to the old buffer need to be reassigned to avoid an use-after-free.	2026-08-28	9.8	CVE-2026-80600
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_irc: fix parse_dcc() off-by-one OOB read parse_dcc() treats data_end as an inclusive end pointer, but its only caller passes data_limit = ib_ptr + datalen, which points one past the last valid byte. The newline search loop iterates while tmp <= data_end, so when no newline is present, *tmp is read at tmp == data_end, one byte beyond the region filled by skb_header_pointer(). irc_buffer is kmalloc'd as MAX_SEARCH_SIZE + 1 bytes and datalen is capped at MAX_SEARCH_SIZE, so the stray read does not fault. The byte is uninitialized or stale; if it contains an ASCII digit, simple_strtoul will consume it and produce a wrong DCC IP or port in the conntrack expectation. The extra allocation byte is also a fragile guard: if the cap or allocation size changes, this becomes a real out-of-bounds read. Change the loop and its post-loop check to use strict less-than, consistent with the caller's exclusive-end convention. Update the function comment accordingly.	2026-08-28	9.1	CVE-2026-80603
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: qede: fix out-of-bounds check for cq->len_list[] Move index check before element access.	2026-08-28	9.8	CVE-2026-80609

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: lwtunnel: Drop skb metadata before LWT encapsulation skb metadata is meant for passing information between XDP and TC. It lives in the skb headroom, immediately before skb->data. LWT programs cannot access the __sk_buff->data_meta pseudo-pointer to metadata. However, LWT encapsulation prepends outer headers, moving skb->data back over the headroom where the metadata sits. On an RX-originated (forwarded) packet that still carries XDP metadata this goes wrong in two different ways, depending on the encap type: 1. Non-BPF LWT encaps (mpls, seg6, ioam6 ...) call skb_push()/skb_pull() and silently overwrite the metadata that sits in the headroom. 2) BPF LWT xmit calls bpf_skb_change_head(), which uses skb_data_move(). That helper expects metadata immediately before skb->data. But since the IP output path runs LWT xmit before neighbour output has built the outgoing L2 header, for forwarded packets skb->data points at the L3 header while skb_mac_header() still points at the old L2 header. skb_data_move() sees metadata ending at skb_mac_header(), not before skb->data, warns and clears metadata: WARNING: CPU: 21 PID: 454557 at include/linux/skbuff.h:4609 skb_data_move+0x47/0x90 CPU: 21 UID: 0 PID: 454557 Comm: napi/iconduit-g Tainted: G O 6.18.21 #1 RIP: 0010:skb_data_move+0x47/0x90 Call Trace: <IRQ> bpf_skb_change_head+0xe6/0x1a0 bpf_prog_...+0x213/0x2e3 run_lwt_bpf.isra.0+0x1d3/0x360 bpf_xmit+0x46/0xe0 lwtunnel_xmit+0xa1/0xf0 ip_finish_output2+0x1e7/0x5e0 ip_output+0x63/0x100 __netif_receive_skb_one_core+0x85/0xa0 process_backlog+0x9c/0x150 __napi_poll+0x2b/0x190 net_rx_action+0x40b/0x7f0 handle_softirqs+0xd2/0x270 do_softirq+0x3f/0x60 </IRQ> That is what happens, as for how to fix it - a received packet that carries metadata can reach an encap through any of the three LWT redirect modes: LWTUNNEL_STATE_INPUT_REDIRECT ip6_rcv_finish dst_input lwtunnel_input LWTUNNEL_STATE_OUTPUT_REDIRECT ip6_rcv_finish dst_input ip6_forward ip6_forward_finish dst_output lwtunnel_output LWTUNNEL_STATE_XMIT_REDIRECT ip6_rcv_finish dst_input ip6_forward ip6_forward_finish dst_output ip6_output ip6_finish_output ip6_finish_output2 lwtunnel_xmit Every encap funnels through the three LWT dispatch helpers, so drop the metadata there, right before handing the skb to the encap op. This single chokepoint covers all encap types and all three redirect modes: - lwtunnel_input(): seg6, rpl, ila, seg6_local - lwtunnel_output(): ioam6 - lwtunnel_xmit(): mpls, LWT BPF xmit Alternatively, we could clear the metadata right after TC ingress hook. That would require a compromise, however. Metadata would become inaccessible from TC egress (in setups where it actually reaches the hook it tact, that is without any L2 tunnels on path).	2026-08-28	9.8	CVE-2026-80612
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: airoha: fix foe_check_time allocation size foe_check_time is declared as u16 pointer but was allocated with only ppe_num_entries bytes instead of ppe_num_entries * sizeof(u16). When airoha_ppe_foe_verify_entry() is called with hash >= ppe_num_entries/2, it writes beyond the allocated buffer, causing heap buffer overflow and potential kernel crash.	2026-08-28	9.8	CVE-2026-80617
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: schfq_codel: Do not call qdisc_tree_reduce_backlog during peek before restoring qlen Whenever fq_codel drops packets during peek, it calls qdisc_tree_reduce_backlog. An issue arises because it calls qdisc_tree_reduce_backlog before it reincrements the qlen. If qlen drops to zero, but peek returns an skb, the parent's qlen_notify callback will be executed even though fq_codel still has 1 packet on the queue and, thus, will mistakenly deactivate the parent's class causing issues like a recent report [1] and a wild memory access in qfq: [29.371146][T360] Oops: general protection fault, probably for non-canonical address 0xfbd59c0000000024: 0000 [#1] SMP KASAN NOPTI [29.371666][T360] KASAN: maybe wild-memory-access in range [0xdead000000000120-0xdead000000000127] [29.371987][T360] CPU: 6 UID: 0 PID: 360 Comm: tc Not tainted 7.1.0-rc5-00285-gc530e5b2dbc6-dirty #82 PREEMPT(full) [29.372384][T360] Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 [29.372620][T360] RIP: 0010:qfq_deactivate_agg (include/linux/list.h:1029 (discriminator 2) include/linux/list.h:1043 (discriminator 2) net/sched/schfq.c:1369 (discriminator 2) net/sched/schfq.c:1395 (discriminator 2)) schfq [29.373544][T360] RSP: 0018:ffff888102417370 EFLAGS: 00010216 [29.373800][T360] RAX: 0000000000000000 RBX: ffff88811224d568 RCX: dffffc0000000000 [29.374079][T360] RDX: 1ffff11021fe1543 RSI: ffff88810ff0aa00 RDI: dffffc0000000000 [29.374368][T360]	2026-08-28	9.8	CVE-2026-80630

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	RBP: ffff88811224c280 R08: dead000000000122 R09: 1bd5a00000000024 [29.374649][T360] R10: fffffbfff7940329 R11: fffffbfff7940329 R12: 0000000000000000 [29.374926][T360] R13: dead000000000100 R14: ffff88811224d580 R15: ffff88811224d578 [29.375207][T360] FS: 00007f5b794e5780(0000) GS:ffff88815d1e9000(0000) knlGS:0000000000000000 [29.375545][T360] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [29.375823][T360] CR2: 000055ffb091f000 CR3: 000000010a305000 CR4: 0000000000750ef0 [29.376103][T360] PKRU: 55555554 [29.376258][T360] Call Trace: [29.376401][T360] <TASK> ... [29.376885][T360] qfq_reset_qdisc (net/sched/sch_qfq.c:357 net/sched/sch_qfq.c:1487) sch_qfq [29.377074][T360] qdisc_reset (net/sched/sch_generic.c:1057) [29.377414][T360] __qdisc_destroy (net/sched/sch_generic.c:1096) [29.377600][T360] qdisc_graft (net/sched/sch_api.c:1062 net/sched/sch_api.c:1053 net/sched/sch_api.c:1159) [29.378593][T360] tc_get_qdisc (net/sched/sch_api.c:1528 net/sched/sch_api.c:1556) Fix this by only calling qdisc_tree_reduce_backlog in peek after the qlen is restored. [1] http://lore.kernel.org/netdev/CAN2cbVe79oj0O9==m4+4x3v+O+qzRagA=2=wkrp9i9=CqYvyZA@mail.gmail.com/			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: avoid num_encaps underflow on bridge VLAN untag The DEV_PATH_BR_VLAN_UNTAG case post-decrements info->num_encaps inside WARN_ON_ONCE(). num_encaps is u8, so if it's already 0 the decrement still happens and wraps it to 255. The break only leaves the inner switch -- a later path entry can set info->indev back to a real device, and we end up returning with num_encaps == 255. nft_dev_forward_path() then walks info.encap[] (size 2) up to num_encaps, which means an OOB stack read and a bogus count copied into the route descriptor. Should only happen on a malformed bridge path stack, hence the WARN, but worth handling sanely. Move the decrement out of the WARN. [While at this, remove the WARN_ON_ONCE since this can only happen with a buggy bridge path stack --pablo].	2026-08-28	9.8	CVE-2026-80634
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_contrack_expect: use conntrack GC to reap expectations This patch replaces the timer API by GC worker approach for expectations, as it already happened in many other subsystems. Use the existing conntrack GC worker to iterate over the local list of expectations in the master conntrack to reap expired expectations. Check IPS_HELPER_BIT to run GC for expectations, set it on for nft_ct expectation which never sets it. Hold the expectation spinlock while iterating over the master conntrack expectation list to synchronize with nf_ct_remove_expectations(). This also performs runtime packet path garbage collection through the expectation insertion and lookup functions while walking over one of the chains of the global expectation hashtables. Unconfirmed conntrack entries are skipped since ct->ext can be reallocated and dying are skipped since those will be gone soon. Set on IPS_HELPER_BIT if the helper ct extension is added, then the new GC worker does not need to bump the ct refcount to check if the ct->ext helper is available. This removes the extra bump on the refcount for expectation timers, this allows to remove several nf_ct_expect_put() calls after the unlink, after this update only removal remains at 1 while on the expectation hashes. This patch implicitly addresses a race with the existing timer API allowing an expectation to access a stale exp->master pointer which has been already released when expectation removal loses races with an expiring timer, ie. timer_del() reporting false. Add a new NF_CT_EXPECT_DEAD flag to reap this expectation via GC. This is needed by nf_contrack_unexpect_related() which is called in error paths to invalidate newly created expectations that has been added into the hashes. These expectations cannot be immediately released as GC or nf_ct_remove_expectations() could race to make it. On expectation insert, the runtime GC reaps stale expectations before checking the expectation limit set by policy. Set current timestamp in nf_ct_expect_alloc(), then add the expectation policy timeout (or custom timeout specified added on top of this) to specify the expectation lifetime.	2026-08-28	9.8	CVE-2026-80668
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: perf tools: Use perf_env__get_cpu_topology() in machine__resolve() machine__resolve() accesses env->cpu[al->cpu].socket_id after checking al->cpu >= 0 and env->cpu != NULL, but without validating al->cpu against env->nr_cpus_avail. Since al->cpu comes from the untrusted perf.data sample, a crafted file with a large CPU index causes an out-of-bounds heap read. Use perf_env__get_cpu_topology() which validates both NULL and bounds. Also bounds-check al->cpu before the cast to struct perf_cpu	2026-08-28	9.1	CVE-2026-80670

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(int16_t): without this, values like 65536 silently truncate to 0, bypassing the accessor's internal check and returning CPU 0's topology.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: perf sched: Fix register_pid() overflow, strcpy, and BUG_ON register_pid() has several issues when processing untrusted perf.data: 1. Integer overflow: (pid + 1) * sizeof(struct task_desc *) can wrap to a small value on 32-bit systems when pid is large (e.g. 0x40000000), causing realloc to return a tiny buffer followed by out-of-bounds writes in the initialization loop. 2. Heap buffer overflow: strcpy(task->comm, comm) copies the untrusted comm string into a fixed 20-byte COMM_LEN buffer with no length check. 3. BUG_ON on allocation failure: perf.data is untrusted input, so allocation failures should be handled gracefully rather than killing the process. 4. Realloc of sched->tasks assigned directly back, leaking the old pointer on failure; nr_tasks incremented before the realloc, leaving corrupted state on failure. Cap pid at PID_MAX_LIMIT (4194304, matching the kernel's maximum on 64-bit), replace strcpy with strncpy, guard against NULL comm, replace BUG_ON with NULL returns using safe realloc patterns, and add NULL checks in callers that dereference the result.	2026-08-28	9.3	CVE-2026-80671
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: bound the look-ahead attribute-list entry in ntfs_external_attr_find() When resolving an attribute lookup with a non-zero @lowest_vcn, ntfs_external_attr_find() peeks at the next \$ATTRIBUTE_LIST entry to decide whether to keep searching, but bounds that not-yet-validated entry only with "(u8 *)next_al_entry + 6 < al_end" (which proves just bytes 0..6 are in range) and "(u8 *)next_al_entry + length <= al_end" with an attacker-controlled, non-8-aligned length. It then reads next_al_entry->lowest_vcn (an __le64 at offset 8) and the name at next_al_entry->name_offset, both of which can lie past al_end -- the exact end of the kvmalloc'd attribute-list buffer (allocated at the on-disk attr_list_size, no rounding). A crafted on-disk \$ATTRIBUTE_LIST whose last entry sits a few bytes before al_end therefore yields a slab out-of-bounds read when the inode is read. Validate the look-ahead entry with ntfs_attr_list_entry_is_valid() (added in patch 1/3) before dereferencing lowest_vcn and the name, so the same fixed-header, length and name bounds the main attribute-list walk uses now guard this read too.	2026-08-28	9.8	CVE-2026-80673
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: validate resident attribute lists and harden the validator A base inode's \$ATTRIBUTE_LIST is sanity-checked by load_attribute_list() only on the non-resident path; ntfs_read_locked_inode() copies a *resident* attribute list into ni->attr_list with a plain memcpy() and no validation at all. Every subsequent walk of ni->attr_list -- ntfs_external_attr_find(), ntfs_inode_attach_all_extents() and ntfs_attrlist_need() -- then trusts the entries are well-formed and reads attr_list_entry fixed-header fields (lowest_vcn at offset 8, mft_reference at offset 16, and the name) with bounds that assume validation already happened. A crafted resident attribute list therefore reaches those walks unvalidated and can drive out-of-bounds reads of the attribute-list buffer. load_attribute_list() itself reads ale->name_offset (offset 7), ale->mft_reference (offset 16) and the name length under only an "al < al_start + size" bound, so its own validation loop can over-read the fixed header of a truncated trailing entry by a few bytes. Factor the per-entry validation into ntfs_attr_list_entry_is_valid(), which requires each entry's fixed header (offsetof(struct attr_list_entry, name)) to be in range before any field is dereferenced, that ale->length is a multiple of 8 covering the fixed header plus the name, and that the entry is in use and carries a live MFT reference. ntfs_attr_list_is_valid() walks the buffer with it and checks the entries tile it exactly. Use the list validator in load_attribute_list() (replacing the open-coded loop, closing its own over-read) and on the resident path in ntfs_read_locked_inode() (which previously skipped validation entirely); patches 2/3 reuse the per-entry helper at the other two attribute-list walks.	2026-08-28	9.8	CVE-2026-80674
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: re-fetch eth header after route_shortcircuit() Before route_shortcircuit(), the eth header pointer is cached from eth_hdr(skb). Inside route_shortcircuit(), pskb_may_pull() can be called, which may reallocate skb->head. In this case, returning to vxlan_xmit() leaves the cached eth pointer pointing to freed memory, leading to a use-after-free when dereferencing eth->h_dest. Fix this by updating eth = eth_hdr(skb) after calling route_shortcircuit().	2026-08-28	9.8	CVE-2026-80681
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: s390: pci: Fix NULL dereference on AIBV allocation failure The airq_iv_create() can return NULL on failure, but the return value was never checked. If it fails, zdev->aibv will	2026-08-28	9.3	CVE-2026-80684

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	be NULL and fail when dereferenced in kvm_zpci_set_irq(). Add a NULL check and free the previously allocated AISB bit and zdev->aisb on failure.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: idpf: bound interrupt-vector register fill to the allocated array idpf_get_reg_intr_vecs() fills the caller-allocated reg_vals[] array from the VIRTCHNL2_OP_ALLOC_VECTORS reply in adapter->req_vec_chunks, bounding its inner loop only by the per-chunk num_vectors. The array is sized separately: idpf_intr_reg_init() allocates kcalloc_objs(struct idpf_vec_regs, total_vecs) from caps.num_allocated_vectors and only checks the returned count after the fill. The sum of per-chunk num_vectors is never reconciled against total_vecs, so a reply with a small num_allocated_vectors but chunks summing higher writes past the end of reg_vals[]. Impact: a control plane (a PF or hypervisor device model) that returns a VIRTCHNL2_OP_ALLOC_VECTORS reply whose per-chunk num_vectors sum exceeds num_allocated_vectors writes struct idpf_vec_regs entries past the end of the reg_vals kmalloc allocation (KASAN slab-out-of-bounds write). Bound the fill loop to the array capacity passed in by the callers, mirroring the sibling idpf_vport_get_q_reg(). The existing num_regs < num_vecs check then rejects an undersized reply without the out-of-bounds write happening first.	2026-08-28	9.3	CVE-2026-80693
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_eth_soc: pass eth to mtk_handle_irq_rx in poll_controller mtk_handle_irq_rx expects a struct mtk_eth * (matching the request_irq cookie), but mtk_poll_controller incorrectly passed the net_device *. Calling ndo_poll_controller with CONFIG_NET_POLL_CONTROLLER enabled would then crash.	2026-08-28	9.8	CVE-2026-80694
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: do not propagate one-packet flag to synced conns Synced connections can be created before their destination exists. When the destination is later added, ip_vs_bind_dest() copies connection flags from the destination into cp->flags. IP_VS_CONN_F_ONE_PACKET connections are not synced. If a synced connection inherits IP_VS_CONN_F_ONE_PACKET while it is already hashed, expiry can treat it as a one-packet connection and skip unlinking the existing conn_tab node, leaving stale hash nodes pointing at a freed struct ip_vs_conn. Drop IP_VS_CONN_F_ONE_PACKET from destination flags when binding synced connections.	2026-08-28	9.8	CVE-2026-80714
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfs: bounds-check buffer log item's dirty bitmap xlog_recover_do_reg_buffer() replays each dirty region described by a buffer log item's bitmap into the buffer read for that item: memcpy(xfs_buf_offset(bp, (uint)bit << XFS_BLF_SHIFT), item->ri_buf[i].iov_base, nbits << XFS_BLF_SHIFT); The destination offset (bit/nbits, from the logged dirty bitmap) and the buffer size (from the logged blf_len) are both attacker-controlled and otherwise unrelated, yet the only thing bounding the copy is an ASSERT(), which compiles away on production kernels. A crafted image logging a small blf_len together with a bitmap bit past the end of that buffer drives the memcpy() past the buffer's allocation, corrupting adjacent kernel heap during mount-time log recovery. This is reachable by anyone who can get a crafted image mounted -- the malicious-filesystem threat model XFS already guards against elsewhere. Turn the ASSERT() into a real XFS_IS_CORRUPT() check that aborts recovery of the buffer with -EFSCORRUPTED, consistent with the validate-and-fail idiom already used in xlog_recover_do_inode_buffer() and xfs_dquot_item_recover.c. xlog_recover_do_reg_buffer() therefore becomes STATIC int and its three callers propagate the error. Found and confirmed with KASAN on a CONFIG_XFS_DEBUG=n build: the crafted image trips a slab-out-of-bounds write before this change and fails recovery cleanly with -EFSCORRUPTED after it.	2026-08-26	8.4	CVE-2026-80536
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Implement a crw lock Unlike the channel_program struct, which covers synchronous I/O submissions and asynchronous interrupts, the CRW region relies exclusively on asynchronous events coming from hardware. Implement a lock to manage the list of those payloads, to ensure they are read cohesively.	2026-08-26	8.8	CVE-2026-80547
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Selectively expand io_mutex The io_mutex was defined to serialize the io_regions, but then has also sort of been associated with the I/O themselves because of the close relationship they share. With the handful of races that are possible, the choices are either to: A) expand the scope of io_mutex to close these remaining	2026-08-26	8.8	CVE-2026-80548

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	windows, or B) reduce the scope of io_mutex to just io_region, and introduce a new lock mechanism for the remaining I/O resources This patch implements A, since B brings with it a lot more interactions that would need to be tracked and kept in a correct hierarchy. It also takes advantage of the workqueue element for cp_free() that now gets called out of fsm_notoper(), which could be invoked out of an interrupt context and thus cannot acquire a mutex itself.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Move cp cleanup out of not operational The fsm_notoper() routine is called when the device has been lost, and is (by definition) no longer operational. Since this can happen asynchronously from the normal behavior of the driver, the cleanup may happen when holding other locks in the calling sequence (notably, the cio subchannel lock). Push the cleanup of the private->cp resources to a workqueue, where it can be done out from under that lock sequence and a future patch can safely manage the locking requirements.	2026-08-26	8.2	CVE-2026-80549
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Ensure index for read/write regions are within range The introduction of the capability chain rightly clamped the region indexes to the range of the capabilities itself, but neglected to do so for the existing read/write regions which should also be enforced.	2026-08-26	8.8	CVE-2026-80552
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Cancel existing workqueues The initialization of the io_work and crw_work workqueues begs the question of whether they should be un-initialized. Add the corresponding cleanup tags in _release_dev to ensure work isn't dispatched after the private struct is free'd.	2026-08-26	8.8	CVE-2026-80553
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Input: focaltech - fix array out-of-bounds in focaltech_process_rel_packet Make finger2 (and also finger1) unsigned, so that if the finger index in the packet is 0 then subtracting 1 creates an array index which overflows above the existing check for FOC_MAX_FINGERS, as the existing comment says it should, instead of writing to state->fingers[-1].	2026-08-26	8.4	CVE-2026-80574
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: reject oversized IBs with per-ring packet limits On GFX rings, amdgpu_cs_p2_ib() passed user-supplied ib_bytes through to ib->length_dw without a limit, while ring_emit_ib() encodes length into packet fields. Oversized values can corrupt adjacent control bits and destabilize command submission. Add a per-ring IB packet size limit helper and reject command submissions exceeding the corresponding dword limit before IB allocation. Use the documented 20-bit limit for GFX/compute/SDMA/VPE, and apply the MM fallback limit for other ring types. (cherry picked from commit 7f48fa2cf62e3fa6c9c3870aa74988f773247e52)	2026-08-26	8.8	CVE-2026-80576
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/qeth: validate user buffer length in SNMP and ARP query ioctls qeth_snmp_command() and qeth_l3_arp_query() allocate a buffer sized by a user-supplied length (udata_len) without checking a lower bound, then set udata_offset to a fixed non-zero value and pass both to a reply callback. The callback bounds-checks the copy with if ((udata_len - udata_offset) < len) Both fields are u32, so a udata_len smaller than udata_offset makes the subtraction wrap and the check pass, and the following memcpy() writes past the allocation. A udata_len of 0 also yields ZERO_SIZE_PTR from kzalloc(), which the existing NULL check does not catch. Reject buffers smaller than udata_offset before allocating, so the callback subtraction can no longer underflow.	2026-08-26	8.4	CVE-2026-80584
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: inet: frags: strip GSO state from fragments before reassembly A virtio_net_hdr (tun/tap, or AF_PACKET with PACKET_VNET_HDR) can mark an IPv4 or IPv6 fragment as GSO; nothing relates gso_type to frag_off. inet_frag_reasm_prepare()/inet_frag_reasm_finish() keep the first fragment's skb as the head of the reassembled datagram, including its shinfo->gso_size/gso_type/gso_segs, and chain the remaining fragments on frag_list with whatever linear/paged layout they arrived with. After ip_defrag() (ip_local_deliver(), nf_defrag_ipv4, ...) the reassembled skb therefore still claims to be GSO (SKB_GSO_DODGY), and the next software segmentation point - udp_rcv_segment() on local delivery, validate_xmit_skb(), or the ip_finish_output_gso() slow path - hands it to skb_segment(). skb_segment()'s frag_list walk assumes GRO-shaped input and hits one of its BUG_ON()'s. Two writes to a tap by an unprivileged user in its own usersns are enough: kernel BUG at	2026-08-28	8.6	CVE-2026-80590

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	net/core/skbuff.c:4899! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI CPU: 0 UID: 1000 PID: 82 Comm: poc Not tainted 7.2.0-pentest+ #2 RIP: 0010:skb_segment+0x20ca/0x48b0 Call Trace: <TASK> __udp_gso_segment+0x29a/0x27d0 udp4_ufo_fragment+0x458/0x6c0 inet_gso_segment+0x429/0x1340 skb_mac_gso_segment+0x233/0x4f0 __skb_gso_segment+0x308/0x660 udp_queue_rcv_skb+0x440/0xad0 udp_unicast_rcv_skb+0xc7/0x2c0 udp_rcv+0x16ce/0x2260 ip_protocol_deliver_rcu+0x197/0x2d0 ip_local_deliver+0x430/0x690 ip_rcv+0x16f/0x1f0 __netif_receive_skb_one_core+0x15e/0x1c0 __netif_receive_skb+0x1e/0x110 netif_receive_skb+0xf6/0x5c0 tun_rx_batched.isra.0+0x3ab/0x790 tun_get_user+0x17c3/0x3550 tun_chr_write_iter+0xba/0x1b0 vfs_write+0x646/0x1130 </TASK> Kernel panic - not syncing: Fatal exception in interrupt This runs with BH disabled, so it is a panic rather than an oops. The same is reachable with CAP_NET_RAW in a netns where a defrag point precedes a GSO point, and from a guest whose VMM forwards virtio_net_hdr to a tap. The SKB_GSO_DODGY frag_list checks added by commit 3dcdbd134f32 ("net: gso: Fix skb_segment splat when splitting gso_size mangled skb having linear-headed frag_list") and by commit 9e4b7a99a03a ("net: gso: fix panic on frag_list with mixed head alloc types") do not cover it: page-backed heads skip them, and kmalloc heads skip them when gso_size == skb_headlen(head), which the sender controls. An skb entering a frag queue is an IP fragment by definition and cannot legitimately carry GSO state: GRO does not merge fragments and the stack segments before it fragments, so only untrusted sources are affected. This has been reachable since commit f43798c27684 ("tun: Allow GSO using virtio_net_hdr"), the first path that let userspace attach GSO metadata to an IP fragment. Reset the GSO fields of every fragment as it is queued, in inet_frag_queue_insert(), which IPv4, IPv6, nf_contrack_reasm and 6lowpan reassembly share; then neither the head nor the frag_list members of the reassembled skb carry them (the members matter too: the ip_do_fragment()/ip6_fragment() fast paths send them out as they are). The head may remain CHECKSUM_PARTIAL; that is already accepted on receive and resolved by skb_checksum_help() in ip_do_fragment()/ip6_fragment() on forward. Tested on top of net.git (dc4b95b8fee9), x86_64: the tap reproducer above, two further IPv4 frag_list geometries that reach BUG_ON(i >= nfrags) and BUG_ON(!list_skb-> head_frag), and an IPv6 fragment-header variant (udp6_ufo_fragment()) each panic the unpatched kernel; with this patch all four datagrams are delivered intact and nothing is logged.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (asus_atk0110) Check package count before accessing element atk_ec_present() walks the management group package returned by the GGRP ACPI method and, for each sub-package, reads its first element: id = &obj->package.elements[0]; if (id-> type != ACPI_TYPE_INTEGER) without checking that the sub-package is non- empty. ACPICA allocates the element array with exactly package.count entries, so for a sub-package with a zero count this reads past the allocation. The sibling function atk_debugfs_ggrp_open() performs the same access but skips empty packages with a package.count check first. Add the same check to atk_ec_present() so a malformed firmware package cannot trigger an out-of-bounds read.	2026-08-28	8.4	CVE-2026-80593
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Input: ims-pcu - only expose sysfs attributes on control interface When the driver was converted to use the driver core to instantiate device attributes (via .dev_groups in the usb_driver structure), the attributes started appearing on all interfaces bound to the driver. Since the ims-pcu driver manually claims the secondary data interface during probe, the driver core automatically creates the sysfs attributes for that interface as well. However, the driver only supports these attributes on the primary control interface. Data interfaces lack the necessary descriptors and internal state to handle these requests, and accessing them can lead to unexpected behavior or crashes. Fix this by updating the is_visible() callbacks for both the main and OFN attribute groups to verify that the interface being accessed is indeed the control interface.	2026-08-28	8.4	CVE-2026-80596
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: dat: ensure accessible eth_hdr proto field When batadv_get_vid() accesses the proto field of the ethernet header, it is not checking if the data itself is accessible. The caller is responsible for it. But in contrast to other call sites, batadv_dat_get_vid() and its caller didn't make sure this is true. This could have caused an out-of-bounds access.	2026-08-28	8.1	CVE-2026-80599

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: gw: acquire ethernet header only after skb realloc The pskb_may_pull() called by batadv_get_vid() could reallocate the buffer behind the skb. Variables which were pointing to the old buffer need to be reassigned to avoid an use-after-free.	2026-08-28	8.8	CVE-2026-80601
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: HID: core: Fix OOB read in hid_get_report for numbered reports When a caller passes a size of 0 to hid_report_raw_event() for a numbered report, the function originally called hid_get_report() before performing any size validation. Inside hid_get_report(), if the report is numbered (report_enum->numbered is true), it unconditionally dereferences data[0] to extract the report ID. With a size of 0, this results in an out-of-bounds read or kernel panic. Fix this by moving the numbered report size validation check before the call to hid_get_report(), ensuring that size is at least 1 before dereferencing the data pointer.	2026-08-28	8.8	CVE-2026-80604
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/amdxdna: Fix iommu domain lifetime race during device removal When force_iova mode is enabled, amdxdna_remove() frees xdna->domain. If amdxdna_gem_obj_free() is called after device removal, it may attempt to access xdna->domain, resulting in a use-after-free. Fix the race by adding freeing xdna->domain as a managed release action, so its lifetime is managed by DRM and remains valid until all managed resources are released.	2026-08-28	8.8	CVE-2026-80608
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: dst_metadata: fix false-positive memcpy overflow in tun_dst_unclone kmalloc_flex() in metadata_dst_alloc() sets __counted_by for the structure to the options_len, which is then initialized to zero. Later, we're initializing the structure by copying the tunnel info together with the options, and this triggers a warning for a potential memcpy overflow, since the compiler estimates that the options can't fit into the structure, even though the memory for them is actually allocated. memcpy: detected buffer overflow: 104 byte write of buffer size 96 WARNING: CPU: X PID: Y at lib/string_helpers.c:1036 __fortify_report skb_tunnel_info_unclone+0x179/0x190 geneve_xmit+0x7fe/0xe00 The issue is triggered when built with clang and source fortification. Fix that by doing the copy in two stages: first - the main data with the options_len, then the options. This way the correct length should be known at the time of the copy. It would be better if the options_len never changed after allocation, but the allocation code is a little separate from the initialization and it would be awkward and potentially dangerous to return a struct with options_len set to a non-zero value from the metadata_dst_alloc(). Another option would be to use ip_tunnel_info_opts_set(), but it is doing too many unnecessary operations for the use case here.	2026-08-28	8.2	CVE-2026-80615
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommufd: Take dma_resv lock before dma_buf_unpin() in release path dma_buf_unpin() requires the caller to hold the exporter's dma_resv lock: void dma_buf_unpin(struct dma_buf_attachment *attach) { ... dma_resv_assert_held(dmabuf->resv); ... } iopt_release_pages() calls dma_buf_unpin() without taking that lock, so every iommufd_ioas_destroy()/iommufd_ioas_unmap() that releases the last reference on a DMABUF-backed iopt_pages triggers a WARN. This was hit while running tools/testing/selftests/iommu/iommufd: WARNING: drivers/dma-buf/dma-buf.c:1137 at dma_buf_unpin+0x62/0x70 RIP: 0010:dma_buf_unpin+0x62/0x70 Call Trace: <TASK> dma_buf_unpin+0x62/0x70 iopt_release_pages+0xe4/0x190 iopt_unmap_iova_range+0x1c7/0x290 iopt_unmap_all+0x1a/0x30 iommufd_ioas_destroy+0x1d/0x50 iommufd_fops_release+0x93/0x150 __fput+0xfc/0x2c0 __x64_sys_close+0x3d/0x80 do_syscall_64+0x65/0x180 </TASK> Take the dma_resv lock around dma_buf_unpin() in iopt_release_pages(), matching the iopt_map_dmabuf() convention. dma_buf_detach() acquires the reservation lock internally, so it must remain outside the locked region.	2026-08-28	8.8	CVE-2026-80633
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: wcn36xx: fix OOB read from short trigger BA firmware response The firmware response length is only checked against sizeof(*rsp) (20 bytes), but when candidate_cnt >= 1, a 22-byte candidate struct is read at buf + 20 without verifying the response contains it. This causes an out-of-bounds read of stale heap data, corrupting the BA session state. Add validation that the response includes the candidate data.	2026-08-28	8.8	CVE-2026-80635
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix out-of-bounds write in ocfs2_remove_refcount_extent [BUG] Unlinking a refcounted file whose refcount tree has leaf blocks triggers a fortify panic due to an out-of-bounds write. [CAUSE] When the last leaf block is removed from a refcount tree,	2026-08-28	8.8	CVE-2026-80638

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ocfs2_remove_refcount_extent() converts the root back to leaf mode with a bulk memset on &rb->rf_records. rf_records sits in an anonymous union with rf_list. rf_list.l_tree_depth aliases rf_records.rl_count, and is 0 for a single-level tree. With rl_count equal to 0, the memset writes past the 16-byte declared size of rf_records, which the fortify checker catches. [FIX] Replace the bulk memset on &rb->rf_records with a correctly-bounded memset on rl_recs[] alone, after setting rl_count to the correct value.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rapidio/tsi721: prevent a bad dereference in tsi721_db_dpc() With a list_for_each() loop, if we don't find the item we are looking for in the list, then the loop exits with the iterator, which is "dbell" in this loop, pointing to invalid memory. This code uses the "found" variable to determine if we have found the doorbell we are looking for or not. However, the problem that the "found" variable needs to be set to false at the start of each iteration, otherwise after the first correct doorbell, then everything is marked as found. Reset the "found" to false at the start of the iteration and move the variable inside the loop.	2026-08-28	8.1	CVE-2026-80645
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: hisi_sas: Add slave_destroy interface for v3 hw WARNING is triggered when executing link reset of remote PHY and rmmmod SAS driver simultaneously. Following is the WARNING log: WARNING: CPU: 61 PID: 21818 at drivers/base/core.c:1347 __device_links_no_driver+0xb4/0xc0 Call trace: __device_links_no_driver+0xb4/0xc0 device_links_driver_cleanup+0xb0/0xfc __device_release_driver+0x198/0x23c device_release_driver+0x38/0x50 bus_remove_device+0x130/0x140 device_del+0x184/0x434 __scsi_remove_device+0x118/0x150 scsi_remove_target+0x1bc/0x240 sas_rphy_remove+0x90/0x94 sas_rphy_delete+0x24/0x3c sas_destruct_devices+0x64/0xa0 [libsas] sas_revalidate_domain+0xe4/0x150 [libsas] process_one_work+0x1e0/0x46c worker_thread+0x15c/0x464 kthread+0x160/0x170 ret_from_fork+0x10/0x20 ---[end trace 71e059eb58f85d4a]--- During SAS phy up, link->status is set to DL_STATE_AVAILABLE in device_links_driver_bound, then this setting influences __device_links_no_driver() before driver rmmmod and caused WARNING. Add the slave_destroy interface to make sure link is removed after flush workque.	2026-08-28	8.4	CVE-2026-80653
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs: fix u16 truncation of restart-area length check ntfs_check_restart_area() validates that the \$LogFile restart area and its trailing log client record array fit within the system page size: u16 ra_ofs, ra_len, ca_ofs; ... ra_len = ca_ofs + le16_to_cpu(ra->log_clients) * sizeof(struct log_client_record); if (ra_ofs + ra_len > le32_to_cpu(rp->system_page_size) ...) return false; ra_len is u16, but the right-hand side is computed in size_t (sizeof(struct log_client_record) == 160). Both ca_ofs and log_clients come straight from the on-disk restart area. With an on-disk log_clients of 410 the product 410 * 160 = 65600; adding ca_ofs and storing into the u16 ra_len truncates modulo 65536 (e.g. ca_ofs 64 gives ra_len 128), so the "fits in the page" check passes even though the client array described by log_clients extends far beyond the page. ntfs_check_log_client_array() then walks the array bounded only by the on-disk log_clients count: cr = ca + idx; if (cr->prev_client != LOGFILE_NO_CLIENT) ... For log_clients 410 it dereferences records up to ca + 409 * 160, ~64 KiB past the kzalloc(system_page_size) restart-page buffer -- an out-of-bounds read of attacker-controlled extent, reachable when a crafted NTFS image is mounted (load_and_check_logfile() at mount time). This is the in-kernel analogue of CVE-2022-30789, fixed in the ntfs-3g userspace driver but never in this revived classic driver. Compute the restart-area length in a u32 so the existing bounds check rejects an over-large client array instead of being defeated by the truncation. Widen ra_ofs and ca_ofs to u32 as well: both are loaded from __le16 on-disk fields and every comparison already promotes to int/size_t, so this changes no result and keeps the declaration uniform.	2026-08-28	8.8	CVE-2026-80672
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: i2c: imx: Fix slave registration race and error handling In i2c_imx_reg_slave(), the slave pointer was assigned before pm_runtime_resume_and_get(). If pm_runtime_resume_and_get() failed, the error path returned without clearing i2c_imx->slave, leaving it non-NULL and causing all subsequent registration attempts to fail with -EBUSY. Additionally, because this driver uses a shared IRQ, the interrupt handler i2c_imx_isr() can execute concurrently and, after acquiring slave_lock, dereference i2c_imx->slave. The previous fix attempt added a lockless i2c_imx->slave = NULL on the error path, but that could race with the ISR under the	2026-08-28	8.4	CVE-2026-80678

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lock and still cause a NULL pointer dereference. Fix both issues by deferring the assignment of i2c_imx->slave and i2c_imx->last_slave_event to after a successful resume, and by performing the assignment inside the slave_lock critical section. This guarantees that the slave pointer is never left stale on the error path and is always valid when observed by the interrupt handler.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: SCO: give the socket its own sco_conn reference sco_conn_del() drops a reference it does not own. It takes one transient reference via sco_conn_hold_unless_zero() and releases it with the sco_conn_put() that follows sco_sock_hold(); the additional put in the !sk branch releases a second one: conn = sco_conn_hold_unless_zero(conn); ... sk = sco_sock_hold(conn); sco_conn_unlock(conn); sco_conn_put(conn); if (!sk) { sco_conn_put(conn); return; } When close() races the controller's Disconnection Complete, sco_chan_del() clears conn->sk and drops the socket's reference while sco_conn_del() is running. sco_conn_del() then sees sk == NULL, its own put drops the count to zero and frees the conn, and the second put writes to the freed kref: BUG: KASAN: slab-use-after-free in sco_conn_put.part.0+0x1a/0x190 Write of size 4 at addr ffff8881099dec74 by task kworker/u17:3/413 Workqueue: hci1 hci_rx_work Call Trace: sco_conn_put.part.0+0x1a/0x190 hci_disconn_complete_evt+0x1ee/0x3e0 hci_event_packet+0x54a/0x650 hci_rx_work+0x321/0x3d0 Allocated by task 413: sco_conn_add+0x72/0x1a0 sco_connect_cfm+0x88/0x670 Freed by task 413: sco_conn_del.isra.0+0x3f/0xf0 hci_disconn_complete_evt+0x1ee/0x3e0 refcount_t: underflow; use-after-free. The root cause is that the socket stores the connection without holding a reference of its own. __sco_chan_add() does: sco_pi(sk)->conn = conn; so the socket borrows whatever reference its caller happened to hold, and the callers paper over that with ad-hoc holds and puts. Give the socket a counted reference instead: __sco_chan_add() takes one and it is released together with the channel (sco_chan_del()) and in sco_sock_destruct(). With the socket holding its own reference, sco_conn_del() no longer needs the extra put and the redundant hold in sco_conn_ready() goes away. Making the socket own its reference means the connection is now actually freed on the error paths of sco_connect() where it used to leak, which in turn runs sco_conn_free() and its hci_conn_drop(conn->hcon). To keep the hci_conn accounting balanced, make that ownership explicit as well: sco_conn_add() consumes one hci_conn reference and the sco_conn owns it for its lifetime. sco_connect() hands over the reference returned by hci_connect_sco() and no longer drops it on the error paths; sco_connect_cfm(), which is not given a reference, takes one with hci_conn_hold() before handing it to sco_conn_add() (and drops it again if the allocation fails); and the explicit hci_conn_hold() in sco_conn_ready() is removed. Every reference then has a single, clear owner.	2026-08-28	8.8	CVE-2026-80683
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: hold conn in hci_connect_acl/le_sync() callbacks There is theoretical UAF if the conn is freed while the hci_sync task is running. Hold refcount to avoid that.	2026-08-28	8.8	CVE-2026-80692
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: spi: spi-qpic-snand: write the feature value before executing SET_FEATURE qcom_spi_send_cmdaddr() programs NAND_FLASH_CMD/NAND_EXEC_CMD and submits the descriptors, which makes the controller execute the command immediately. For SPINAND_SET_FEATURE the value to be written is only placed into NAND_FLASH_FEATURES afterwards, by qcom_spi_io_op(), in a second submission - so the chip is programmed with whatever that register happened to hold from a previous operation, and the intended value is only applied by the *next* SET_FEATURE. Measured on a TP-Link Archer AX55 v1 (IPQ5018, ESMT F50L1G41LB): writing 0x40 to the configuration register (0xb0) leaves the chip at 0x00, and the subsequent write of 0x00 leaves it at 0x40 - every write lands one operation late. This stayed unnoticed until v6.18 added SPI-NAND OTP support together with OTP entries for ESMT chips. spinand_otp_rw() enables OTP mode, reads, and disables it again, and mtd_otp_nvmem_add() does this during MTD registration. With the off-by-one, the "disable" write actually applies the previously requested value, so CFG_OTP_ENABLE ends up set: the chip stays in OTP mode, every subsequent array read returns the OTP area instead of the array (UBI reports an empty device) and all writes fail with -EIO because the OTP area is write protected. On this board that makes the whole flash unusable and the device unbootable. Write the feature value into NAND_FLASH_FEATURES as part of the same transaction, before NAND_EXEC_CMD. While at it, copy only the bytes the operation actually carries - the previous code dereferenced a 4-byte pointer on a	2026-08-28	8.4	CVE-2026-80712

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	one-byte buffer (spinand->scratchbuf). With this patch the flash contents read back bit-identical to a known-good dump of the same board taken under the vendor firmware (md5-verified across partitions), and writes work.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: io_uring: preserve task restrictions across exec Per-task restrictions apply to all rings created by a task. Once installed, they should not be dropped across exec. For a task that has used io_uring, the exec cancellation path calls __io_uring_free(). This frees both the task context and the per-task restriction, so a ring created after exec is unrestricted. Split task context cleanup into io_uring_free_tctx(), and use it from the exec cancellation path. Keep __io_uring_free() for final task cleanup, where both the context and restriction are released.	2026-08-28	8.4	CVE-2026-80713
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: ensure no dangling hcon references in iso_conn After iso_conn_del(), ISO sockets should not dereference the hcon any more. Currently, clearing iso_conn::hcon relies on iso_conn_del() releasing the last reference to the iso_conn. Simplify this by explicitly clearing conn->hcon in iso_conn_del(), to avoid more complex reasoning on races about who holds the last reference.	2026-08-28	8.8	CVE-2026-80721
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: validate individual TWT params before driver setup ieee80211_process_rx_twt_action() only partially validates a received S1G TWT setup frame before queueing it. An individual agreement can therefore reach ieee80211_s1g_rx_twt_setup() with twt->length too short for the full struct ieee80211_twt_params. The individual path passes twt to drv_add_twt_setup(). Both the tracepoint and the driver callback consume the complete parameters block, not merely req_type. Do not pass a short individual agreement to the driver. Broadcast agreements remain unchanged because they are rejected locally after accessing only req_type. [edit commit message to not overclaim lack of validation nor understate driver impact]	2026-08-28	8.8	CVE-2026-80722
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: of: reserved_mem: prevent OOB when too many dynamic regions are defined On boot, fdt_scan_reserved_mem() saves each dynamically-placed /reserved-memory subnode into a local array of size MAX_RESERVED_REGIONS. If the device tree defines more than MAX_RESERVED_REGIONS dynamically-placed regions, fdt_scan_reserved_mem() writes past the end of the local array. Add a bounds check that logs an error and skips the excess regions, restoring the original behavior.	2026-08-28	8.4	CVE-2026-80723
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ptp: vmclock: prevent read-only mappings from becoming writable vmclock_miscdev_mmap() rejects writable mappings of the shared vmclock ABI page with -EROFS, but leaves VM_MAYWRITE set. Userspace can map the page read-only and then upgrade it to writable with mprotect(), after which the guest can corrupt the host-written timekeeping data (sequence counter, UTC time, TSC offset) that the vmclock ABI defines as read-only. Clear VM_MAYWRITE on the read-only path so the mapping cannot be upgraded, as i915 does for its read-only objects and as fixed in drm/vc4 (CVE-2026-68445) and drm/panthor (CVE-2024-53071).	2026-08-28	8.8	CVE-2026-80724
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_bpf: reject dev-bound programs bound to a different device cls_bpf_prog_from_efd() obtained a SCHED_CLS program via bpf_prog_get_type_dev() but never verified that a device-bound (offloaded) program's bound netdev matches the TC netdev the classifier is being attached to. This let a program loaded with prog_ifindex for device A be attached via cls_bpf + skip_sw to device B; deleting device A then destroyed the program's offload state while it was still attached to device B, triggering a netdevsim WARN (panic with panic_on_warn=1). Mirror the XDP attach path (net/core/dev.c) and reject the attach with -EINVAL when a dev-bound program's bound device does not match the target device.	2026-08-26	7.8	CVE-2026-74736
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_u32: skip hash tables in u32_bind_class() u32_walk() enumerates both struct tc_u_hnode and struct tc_u_knode through the walker callback. u32_bind_class() unconditionally casts the passed fh to tc_u_knode and accesses &n->res, so when fh is actually a tc_u_hnode, which has no tcf_result member, this results in a slab-out-of-bounds read of res->classid in tc_cls_bind_class(). The issue can be reproduced with the following commands: tc qdisc add dev lo root handle 1: hfsc tc class add dev lo parent 1: classid 1:1 hfsc sc rate 1000kbit tc filter add dev lo parent	2026-08-26	7.8	CVE-2026-74739

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1:1 protocol ip prio 1 u32 match u32 0 0 flowid 1:1 tc class add dev lo parent 1: classid 1:2 hfsc sc rate 2000kbit Fix this by skipping hash tables via the TC_U32_KEY(handle) check.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ngbe: fix NULL pointer dereference in non-MSI-X interrupt enabling In non-MSI-X mode (such as legacy INTx or single MSI), wx->msix_entry is not allocated or initialized. Calling NGBE_INTR_MISC(wx) dereferences wx->msix_entry->entry, leading to a NULL pointer dereference crash. This issue was introduced by fixing the IRQ vector when the number of VFs is 7. Fix the issue by explicitly checking `pdev->msix_enabled` to determine the correct vector index. Additionally, as a side fix, set the interrupt mask to BIT(0) for the non-MSI-X fallback. In MSI/INTx mode, the MISC and queue interrupts share vector 0, and the WX_PX_MISC_IVAR register is only valid in the MSI-X case. Thus, BIT(0) is the correct mask for the miscellaneous cause when MSI-X is disabled.	2026-08-26	7.5	CVE-2026-74741
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: veth: fix queue index used to wake the peer txq in veth_poll veth_poll() derives the index of the peer TX queue to wake from rq->xdp_rxq.queue_index. That field is only initialized by xdp_rxq_info_reg() in veth_enable_xdp_range(), which runs only when an XDP program is attached. On the plain GRO/NAPI path (veth_napi_enable_range()) xdp_rxq_info_reg() is never called, so queue_index stays 0 for every queue, as priv->rq is zero-allocated. So in a multi-queue setup with GRO enabled and no XDP program attached, every NAPI instance looks at the peer's TX queue 0. If veth_xmit() stops peer TX queue 1 because the ptr_ring is full (NETDEV_TX_BUSY), nothing ever wakes it again: the poller draining queue 1 wakes queue 0 instead. veth implements no ndo_tx_timeout, so the netdev watchdog does not kick in either, and the queue stays stopped indefinitely. Derive the index from the position of the rq within priv->rq instead, which is correct regardless of whether XDP was ever enabled. Scripts to reproduce the stall are available at https://github.com/netoptimizer/veth-backpressure-performance-testing	2026-08-26	7.5	CVE-2026-74742
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: eth: bnxt: avoid deadlock when canceling IRQ affinity notifier Unregistering IRQ affinity notifiers waits for the callback synchronously. bnxt takes the netdev instance lock in the notifier (to restart the queue) and cancels the work under the same lock. This may obviously deadlock. Move the restart to the async service task. The queue restart isn't super time sensitive. Store the new TPH tag, schedule the task. Safely canceling the service task is already ironed out. In bnxt_request_irq() the order of registering notifier, affinity and initial TPH programming has to be inverted. I think it was racy previously since user may trigger an update as soon as notifier is installed. There's a small known gap - if pcie_tph_get_cpu_st() fails at init and the target tag is 0 we may miss programming the entry. This does not seem worth fixing, the code has skip-on-failure all over the place, anyway.	2026-08-26	7.5	CVE-2026-74745
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: revalidate ihl to prevent out-of-bounds access While the outer IP header is already pulled into the skb head, we must be careful and revalidate the embedded headers after reading them from the skb frags to prevent out-of-bounds access. One such place reported by Sashiko is ip_vs_nat_icmp() where local process can change the ihl field and after skb_ensure_writable() we can see larger value which is a problem for the ip_send_check(cih) calls. Add check to drop the packet if the ihl field is changed.	2026-08-26	7.8	CVE-2026-74747
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: fix refcount race between list:set GC and swap __ip_set_put_byindex() resolved the index to a set pointer under RCU, then took ip_set_ref_lock in __ip_set_put() to decrement set->ref. ip_set_swap() holds that same lock while swapping both the ip_set_list slots and the two sets' ref counters, so it can interleave between the dereference and the lock acquisition, leaving the caller to decrement a set whose reference already moved to the other index and hit BUG_ON(set->ref == 0). list_set_gc() reaches this from timer softirq, which the nfnl mutex does not serialize against swap: an expiring list:set member calls list_set_del() -> ip_set_put_byindex() while IPSET_CMD_SWAP runs on the referenced sets. Resolve the index and decrement under ip_set_ref_lock, as ip_set_swap() already does, keeping the refcount tied to the index rather than to a stale set pointer. kernel BUG at net/netfilter/ipset/ip_set_core.c:685! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI RIP: 0010:ip_set_put_byindex (net/netfilter/ipset/ip_set_core.c:870) Call Trace: <IRQ> list_set_del (net/netfilter/ipset/ip_set_list_set.c:159) set_cleanup_entries	2026-08-26	7.8	CVE-2026-74748

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(net/netfilter/ipset/ip_set_list_set.c:181) list_set_gc (net/netfilter/ipset/ip_set_list_set.c:578) call_timer_fn (kernel/time/timer.c:1748) __run_timers (kernel/time/timer.c:1799 kernel/time/timer.c:2374) run_timer_softirq (kernel/time/timer.c:2405) </IRQ> Kernel panic - not syncing: Fatal exception in interrupt			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ovpn: defer key slot crypto freeing to workqueue Key slots are released through a kref and the existing release path frees the AEAD transforms from an RCU callback. That is not safe for all crypto implementations: crypto_free_aead can sleep, for example when an async or hardware implementation has teardown work to complete. Use queue_rcu_work for key-slot release. This keeps the RCU grace period needed by lockless key-slot readers, but runs the actual crypto teardown from workqueue context where sleeping is allowed. Once the rcu_work callback runs, pre-existing RCU readers are gone, and the final kref put already proves that no transform user remains, so the worker can release the AEAD transforms and free the slot directly. The previous patch drains ovpn_wq during module exit, so queued key-slot teardown work cannot outlive module text.	2026-08-26	7.5	CVE-2026-74750
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: perf: Reject exited events as group leaders perf_event_remove_on_exec() sets remove-on-exec events to the EXIT state and detaches their group relationships. The event's file descriptor can remain open, however, and perf_event_open() currently accepts that event as a group leader because its early validation rejects only REVOKED and DEAD events. A new sibling can consequently be linked to the detached leader. When the leader is closed, perf_group_detach() observes that its PERF_ATTACH_GROUP bit is already clear and skips the new sibling. The sibling then retains a group_leader pointer to the freed event. Reject group leaders in the EXIT state. Perform the check while holding the shared context mutex so that an exec in the target task cannot detach the leader between validation and group attachment. [peterz: make the earlier test fully consistent]	2026-08-26	7.8	CVE-2026-74753
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ovpn: fix NULL dereference when killing missing key ovpn_crypto_kill_key assumes both crypto slots are populated and dereferences each slot before checking it. That is not guaranteed: a peer can have only one installed key, and the kill path may be asked to remove a key that is not present. Read each slot once while holding the crypto state lock, check for NULL before looking at key_id, and only replace the slot that actually matches.	2026-08-26	7.5	CVE-2026-80520
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: af_unix: Unlink scc_entry in unix_del_edge(). Kyle Zeng reported that GC could free a dead SCC partially. The scenario is as follows: 1) Create two SCCs: X -. A <-> B ^--' 2) Run the following concurrently: 2-1) send() sk-B to sk-B from sk-X 2-2) close() both A and B At 2-1), there is a small window where unix_add_edges() publishes a new edge (B <-> B) to GC but its skb is not queued by skb_queue_tail(). If 2-2) completes before skb_queue_tail() and GC is triggered, it judges A <-> B as dead, but B is not freed because GC cannot collect the not-yet-queued skb holding the B <-> B edge. X -. A <-> B -. This edge is visible ^--' ^..'^ but skb is not This itself is not a problem since the next GC run will judge B as dead as well and free it finally. X -. A <.> B -. ^--' ^--' However, X's SCC forces the next GC to call unix_walk_scc_fast(), and it iterates over A through B's scc_entry. Let's unlink scc_entry before freeing the vertex in unix_del_edge().	2026-08-26	7.8	CVE-2026-80521
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: tegra - fix rctx->cryptlen calculation in tegra_gcm_do_one_req() Perform rctx->cryptlen calculation in tegra_gcm_do_one_req() the same way it is done in tegra_ccm_crypt_init(). The current formulae may lead to a crash if a caller does not call tegra_gcm_setauthsize() and so ctx->authsize remains zero. Then a decrypt operation with incorrect rctx->cryptlen will lead to a write beyond rctx->dst_sg buffer. As a follow-up cleanup delete struct tegra_aead_ctx->authsize field since it appears to be completely unused. Also simplify tegra_ccm_setauthsize() and tegra_gcm_setauthsize() functions respectively.	2026-08-26	7.8	CVE-2026-80522
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: clk: spacemit: k3: set hdma clock as critical HDMA clock is responsible for the internal TCM access path of X100 RISC-V core, so set the clock flag as critical to prevent it from being shut off, otherwise the Linux system will hang, for example in the case of a vector instruction access generates a page fault.	2026-08-26	7.1	CVE-2026-80523

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: tas2562: Validate values for volume writes tas2562_volume_control_put() does not do any validation of the control value written by userspace, it uses it to look up a value in a fixed size array which can easily be overflowed and then writes whatever value it gets back to the device. Add validation that we are loading a value we have in the array.	2026-08-26	7.8	CVE-2026-80526
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ceph: fix hanging __ceph_get_caps() with stale mds_wanted A reader can hang forever in __ceph_get_caps() when the client no longer holds 'FILE_RD', but local cap state still says that the capability is already wanted (via 'mds_wanted'). One way to trigger this is through MDS cap revocation. If another client performs a conflicting operation, the MDS can revoke 'FILE_RD' from the reader; the next read then has to reacquire 'FILE_RD'. If the cap update that should request 'FILE_RD' never reaches the MDS after 'cap->mds_wanted' was raised, the reader is left holding only non-file caps while local 'mds_wanted' still includes the file read caps. In that state, try_get_cap_refs() sees 'need <= mds_wanted' and returns 0, so __ceph_get_caps() just waits on 'i_cap_wq'. If the cap update that was supposed to request 'FILE_RD' never reaches the MDS after 'cap->mds_wanted' was raised, no further request is sent and the waiter can sleep indefinitely until unrelated cap traffic happens to wake it up. The ordering issue is that 'cap->mds_wanted' is updated in __prep_cap() before the 'CEPH_MSG_CLIENT_CAPS' message is actually queued for send. That makes one field serve two different meanings at once: what this client wants, and what the client believes the MDS already knows it wants. A proper fix would be to split those states and track whether a cap update is actually in flight or has been observed by the MDS. However, simply moving the 'cap->mds_wanted' assignment later would not be sufficient: queueing the message in the messenger does not guarantee that the MDS processed that specific wanted set, and reconnect or message loss can still invalidate that assumption. Fixing that properly would require a larger rework of the cap state machine. To allow simpler backports to stable kernels, this patch implements a simpler workaround: - stop waiting forever in __ceph_get_caps(); after a bounded wait, fall back to the renew path - make ceph_renew_caps() issue a synchronous 'OPEN' request whenever the inode still does not actually hold the wanted caps, instead of only calling ceph_check_caps() The extra issued-vs-wanted check in ceph_renew_caps() is necessary because the previous test only checked whether the inode still had any real caps at all. That is not enough after revocation: the client can still hold something like 'pLs' and yet be missing 'FILE_RD' completely. In that case, falling back to ceph_check_caps() is not sufficient, because it still trusts 'cap->mds_wanted' and may resend nothing. By requiring '(issued & wanted) == wanted' before taking the asynchronous path, the code only uses ceph_check_caps() when the 'wanted caps' are already actually issued. Otherwise, it sends the synchronous 'OPEN' renew. This preserves the existing asynchronous fast path when the wanted caps are already issued, avoids changing cap-state semantics, and fixes the hang by guaranteeing that a stalled waiter eventually retries through a path that does not rely on the stale 'mds_wanted' state. [idryomov: move CEPH_GET_CAPS_WAIT_TIMEOUT from libceph.h to mds_client.h, formatting]	2026-08-26	7.5	CVE-2026-80527
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfs: fix exchange-range reflink flag clearing issue with INO1_WRITTEN When exchanging two full-file ranges, xmi_can_exchange_reflink_flags() can move the reflink inode flag from the file that currently has it to the other file, as long as exactly one side is marked. This assumes that the file contents, and therefore all shared extents, are exchanged. That assumption is not true when XFS_EXCHMAPS_INO1_WRITTEN is set. xfs_exchmaps_can_skip_mapping() can skip hole and unwritten mappings from file1, so an exchange can complete without moving every mapping that the earlier flag-swap decision accounted for. In that case the post-operation cleanup can clear the reflink flag from an inode that still owns shared written extents. Later writes then take the non-reflink write path and may update blocks that should still have been protected by CoW, which shows up as data corruption between reflink-related files. Fix this by disabling the reflink flag exchange whenever XFS_EXCHMAPS_INO1_WRITTEN is requested. The contents exchange can still proceed; the conservative outcome is that both inodes keep the reflink flag. The regular reflink flag cleanup path can drop the extra flag later once the inode no longer has shared extents.	2026-08-26	7.1	CVE-2026-80530

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfs: avoid UAF on sc->tempip in xrep_tempfile_create LOLLM noticed a potential UAF if the tempfile creation code fails after it set sc->tempip. Fix that.	2026-08-26	7.8	CVE-2026-80531
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfs: fix off-by-one in rtrefcount btree root level validation xfs_rtrefcountbt_compute_maxlevels() sets mp->m_rtrefc_maxlevels = min(d_maxlevels, r_maxlevels) + 1; where the trailing "+ 1" already accounts for the inode-root level, so the deepest valid on-disk root level is m_rtrefc_maxlevels - 1 and a cursor must satisfy bc_nlevels <= bc_maxlevels (= m_rtrefc_maxlevels). The two on-disk validation paths, xfs_rtrefcountbt_verify() and xfs_ifformat_rtrefcount(), check the root level with ">" instead of ">=", so a crafted rtreflink (metadir + realtime + reflink) image whose /rtgroups/N.refcount inode has bb_level == m_rtrefc_maxlevels is accepted on mount. xfs_rtrefcountbt_init_cursor() then sets bc_nlevels = bb_level + 1, exceeding bc_maxlevels by one. Since the xfs_rtrefcountbt_cur slab object is sized for exactly bc_maxlevels entries, the first btree op on such a cursor indexes bc_levels[m_rtrefc_maxlevels] past the end of the object. This is reached by the first rtrefcount cursor built after mount, via log/CoW recovery (xfs_reflink_recover_cow() during xfs_mountfs()) or an FS_IOC_GETFSMAP over the realtime device. Reject a root level equal to m_rtrefc_maxlevels, matching the ">=" form already used by the sibling data-device refcount/rmap verifiers and the in-memory rtrmap verifier. BUG: KASAN: slab-out-of-bounds in xfs_btree_lookup (fs/xfs/libxfs/xfs_btree.c:2101) Write of size 2 at addr ffff888018391658 by task exploit/144 xfs_btree_lookup (fs/xfs/libxfs/xfs_btree.c:2101) xfs_btree_query_range (fs/xfs/libxfs/xfs_btree.c:5308) xfs_refcount_recover_cow_leftovers (fs/xfs/libxfs/xfs_refcount.c:2113) xfs_reflink_recover_cow (fs/xfs/xfs_reflink.c:1085) xlog_recover_finish (fs/xfs/xfs_log_recover.c:3551) xfs_mountfs (fs/xfs/xfs_mount.c:1158) xfs_fs_fill_super (fs/xfs/xfs_super.c:1940) get_tree_bdev_flags (fs/super.c:1634) vfs_get_tree (fs/super.c:1694) path_mount (fs/namespace.c:4161) __x64_sys_mount (fs/namespace.c:4367) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) The buggy address belongs to the cache xfs_rtrefcountbt_cur of size 216 The buggy address is located 8 bytes to the right of allocated 216-byte region [ffff888018391578, ffff888018391650) Kernel panic - not syncing: Fatal exception	2026-08-26	7.8	CVE-2026-80537
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfs: propagate errors from xfs_rtginode_load xfs_rtginode_ensure() treats every xfs_rtginode_load() error other than -ENOENT as success. This can leave the realtime group inode unset after an I/O, allocation, or corruption error. Growfs then continues as though the inode had been loaded. Only -ENOENT means that the inode needs to be created. Return all other errors to the growfs caller.	2026-08-26	7.1	CVE-2026-80538
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix UVD decode image min size calculation This needs to use pitch instead of width. Also reject pitch over 4096 to avoid overflow. (cherry picked from commit b41c8cb12e202b220353332ab87dc01a11f69304)	2026-08-26	7.8	CVE-2026-80540
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: validate GEM_CREATE domain combinations AMDGPU_GEM_CREATE checked domain bits against AMDGPU_GEM_DOMAIN_MASK, but did not validate domain combinations. Userspace could combine CPU GTT VRAM with DOORBELL, GDS, GWS, or OA, making amdgpu_bo_placement_from_domain() exceed AMDGPU_BO_MAX_PLACEMENTS and hit BUG_ON(). Allow combinations only within CPU/GTT/VRAM, and require non-CPU/GTT/ VRAM domains to be specified one at a time. Return -EINVAL for invalid combinations in amdgpu_gem_create_ioctl(). v2: Rename helper from amdgpu_gem_domain_valid() to amdgpu_gem_are_domains_valid() (Christian) (cherry picked from commit db39852d0c39843cb02048dfb47e4b8c703e9080)	2026-08-26	7.8	CVE-2026-80541
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Improve EP11 CPRB domain handling with ASN.1 parsing The zcrypt_msgtype6_send_ep11_cprb() function uses fragile struct overlays to access and modify the domain field in the EP11 CPRB payload, creating maintainability and security concerns: 1. Struct overlay approach (pld_hdr) assumes fixed payload structure and doesn't validate the actual ASN.1 encoding. 2. Complex length format detection logic is error-prone and doesn't properly validate bounds at each parsing step. 3. Direct struct member access bypasses proper ASN.1 validation. Fix by replacing struct overlays with explicit ASN.1 parsing that validates each field (payload tag/length, function tag/length/value, optional domain tag/length/value)	2026-08-26	7.8	CVE-2026-80544

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with proper bounds checking at every step. Add <code>asn1_int_encode()</code> helper function to safely write integer values with correct endianness conversion. This makes the code consistent with the validation pattern introduced with the rework of the <code>xcrb_msg_to_type6_ep11cprb_msgx()</code> function.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Improve EP11 CPRB length and overflow checks The <code>xcrb_msg_to_type6_ep11cprb_msgx()</code> function lacks proper input validation, creating security vulnerabilities: 1. Missing minimum size validation: The <code>ep11_cprb</code> structure and subsequent payload fields (<code>pld_tag</code> , <code>pld_lenfmt</code>) are copied from userspace without verifying sufficient buffer length. 2. Arithmetic overflow in length calculations: CEIL4 alignment could overflow, bypassing size checks and enabling buffer overflows. 3. The payload is <code>asn1</code> encoded but the function just uses a simple <code>c struct</code> overlay to access some fields of the payload. Fix by using <code>size_t</code> for length calculations, adding <code>U32_MAX</code> boundary checks after alignment, and validating minimum request size and minimum reply size before copying from userspace. Do a very simple <code>asn1</code> parsing of the payload up to the function value field.	2026-08-26	7.8	CVE-2026-80545
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Improve CCA CPRB length and overflow checks The <code>xcrb_msg_to_type6cprb_msgx()</code> function lacks proper input validation, creating security vulnerabilities: 1. Integer overflow after CEIL4 alignment: Signed int variables could overflow during 4-byte boundary alignment, causing undersized buffer allocations or incorrect bounds checking. 2. Missing minimum size validation: The <code>CPRBX</code> structure is copied from userspace without verifying sufficient buffer length. Undersized buffers cause uninitialized memory access when reading structure fields like <code>cprbx.cprb_len</code> and <code>cprbx.domain</code> . 3. Arithmetic overflow in sum calculations: Adding control block and data block sizes could overflow, bypassing size checks and enabling buffer overflows. Fix by using <code>size_t</code> for length calculations, adding <code>U32_MAX</code> boundary checks after alignment, validating minimum control block size before copying from userspace, and detecting sum calculation overflows.	2026-08-26	7.8	CVE-2026-80546
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Fix out of bounds check on CCW array The routine <code>ccwchain_calc_length()</code> counts the number of channel command words (CCWs) that are chained together in a single channel program, and rejects anything larger than <code>CCWCHAIN_LEN_MAX</code> (256) CCWs. The loop itself is "do..while (count < 257)", and while the logic in <code>is_cpa_within_range()</code> correctly adjusts between the 0-index array of CCWs and the count of CCWs starting at 1, this means it would look at a possible 257th CCW before ending the loop and (correctly) returning an error. Fix this by restructuring the loop to break as soon as 256 CCWs (thus indexes 0-255) are examined, without looking at memory outside the range.	2026-08-26	7.9	CVE-2026-80550
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/vfio_ccw: Free all memory if <code>cp_init()</code> fails The routine <code>cp_free()</code> is called to unpin/free any memory once an I/O is completed successfully, or if <code>cp_prefetch()</code> fails. But if <code>cp_init()</code> fails, and <code>cp->initialized</code> is not enabled, the same routine cannot be used to free all the memory. An attempt to address this exists in <code>ccwchain_handle_ccw()</code> , where a single call to <code>ccwchain_free()</code> is made for the currently-processed CCW segment. But this will leak other segments (created as a result of a Transfer in Channel) that had been allocated as part of the same channel program. Address this by performing the cleanup outside of the recursive <code>ccwchain_handle_ccw()/ccwchain_loop_tic()</code> logic.	2026-08-26	7.1	CVE-2026-80555
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mmc: atmel-mci: Fix use-after-free in <code>atmci_remove</code> due to race condition In <code>atmci_probe</code> , <code>&host->bh_work</code> is bound with <code>atmci_work_func</code> , and <code>atmci_interrupt</code> , <code>atmci_timeout_timer</code> and <code>atmci_dma_complete</code> can all queue this work on <code>system_bh_wq</code> . If we remove the module, <code>atmci_remove</code> makes cleanup and the memory allocated for host with <code>devm_kzalloc()</code> is released after the remove callback returns, while the work mentioned above may still be pending or running. The sequence of operations that may lead to a UAF bug is as follows: CPU0 CPU1 <code>atmci_interrupt</code> <code>queue_work(system_bh_wq, &host->bh_work)</code> <code>atmci_remove</code> <code>atmci_cleanup_slot(...)</code> <code>atmci_writel(host, ATMCI_IDR, ~OUL)</code> <code>timer_delete_sync(&host->timer)</code> <code>dma_release_channel(host->dma.chan)</code> <code>free_irq(platform_get_irq(pdev, 0), host)</code> <code>atmci_work_func</code> // use host // <code>devm</code> resources released after // remove returns, host is freed // use host (use-after-free) Fix it by canceling the work after all the sources that can schedule	2026-08-26	7.8	CVE-2026-80556

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	it (IRQ handler, timeout timer and DMA completion callback) have been stopped, and before proceeding with the remaining cleanup in atmc_i_remove.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Input: sur40 - fix input device registration ordering In sur40_probe(), input_register_device() was previously called early before the V4L2 video device and vb2_queue components were fully initialized. If userspace opened the input device immediately upon registration, sur40_open() would trigger and start the sur40_poll() worker thread. This worker thread invokes sur40_process_video() and accesses the uninitialized vb2_queue structure, leading to a data race and potential system crash. Furthermore, if V4L2 or video registration failed after input_register_device() succeeded, the error path fell through to calling input_free_device() on a successfully registered device instead of input_unregister_device(), corrupting input core state. Move input_register_device() to the very end of sur40_probe(). This ensures the V4L2 and video queue structures are fully initialized before polling can start, and naturally resolves the error path bug since input_free_device() is now only called when input registration has not yet occurred. To maintain strict LIFO (Last-In, First-Out) teardown ordering, also move input_unregister_device() to the very beginning of sur40_disconnect(). This guarantees that the input polling worker thread is stopped before V4L2 video components or control handlers are unregistered.	2026-08-26	7.8	CVE-2026-80559
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: openrisc: signal: do not restore privileged SR bits on sigreturn restore_sigcontext() copies the whole supervision register (SR) from the signal frame and only clears SPR_SR_SM before the value is reloaded into the hardware SR (through ESR and l.rfe) on the return to user space. All other SR bits are left under user control. An unprivileged task can thus return from a signal handler through a crafted sigframe that clears SPR_SR_DME. With the data MMU disabled the CPU performs no translation or protection on data accesses, so the task gains read and write access to arbitrary physical memory, a local privilege escalation. SPR_SR_IME, SPR_SR_SUMRA, SPR_SR_LEE, SPR_SR_EPH and the cache-enable bits are exposed the same way. The ptrace GPR regset already refuses any change to SR for exactly this reason. Restore only the arithmetic flag bits (F, CY, OV) from the signal frame and take every privileged control bit from the SR the kernel saved on signal entry. Verified with qemu-system-or1k -M or1k-sim: before this change an unprivileged PoC clears SPR_SR_DME in rt_sigreturn and writes a marker to physical address 0x03000000 (beyond the kernel's mem=32M); afterwards the same PoC receives SIGSEGV and physical memory is unchanged.	2026-08-26	7.8	CVE-2026-80560
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: qce - fix error path in devm_qce_register_algs If ops->register_algs() fails, the error path repeatedly calls the same ops->unregister_algs() from the failed registration. Use the loop index to unregister the previously registered algorithms instead.	2026-08-26	7.8	CVE-2026-80565
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Input: synaptics-rmi4 - block s_input when F54 queue is busy Changing the input (diagnostic report type) mid-stream changes the report size. Since V4L2 buffers are allocated based on the size at stream start, changing the input while streaming could lead to a heap buffer overflow if the new size is larger than the allocated buffers. Prevent this by blocking VIDIOC_S_INPUT with -EBUSY if the V4L2 queue is busy (streaming).	2026-08-26	7.8	CVE-2026-80568
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Input: synaptics-rmi4 - bound the F54 report size to the allocated buffer rmi_f54_work() reads a diagnostics report from the device into f54->report_data, sizing the transfer with rmi_f54_get_report_size(): report_size = rmi_f54_get_report_size(f54); ... for (i = 0; i < report_size; i += F54_REPORT_DATA_SIZE) { int size = min(F54_REPORT_DATA_SIZE, report_size - i); ... rmi_read_block(..., f54->report_data + i, size); } report_data is allocated once at probe from F54's own electrode counts (array3_size(f54->num_tx_electrodes, f54->num_rx_electrodes, sizeof(u16))), but rmi_f54_get_report_size() computes the size from drv_data->num_*_electrodes when those are set, i.e. from the F55 function's electrode counts. Both counts come straight from device queries (F54 and F55 each report up to 255 electrodes) and nothing constrains the F55 counts to the F54 ones. A malicious or malfunctioning RMI4 device that reports larger F55 electrode counts than its F54 counts makes report_size exceed the allocation, so the read loop writes past report_data (and the V4L2 dequeue memcopy() then reads past it). On conforming hardware the F55 configured electrodes are a subset of the F54 physical electrodes, so report_size never exceeds the buffer and well-behaved	2026-08-26	7.8	CVE-2026-80569

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	devices are unaffected. Record the allocation size and reject a report that does not fit, mirroring the existing zero-size check.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Input: synaptics-rmi4 - zero report size on F54 work error In rmi_f54_work(), if an error occurs during report request or command verification, the code jumped directly to the 'error' label, bypassing the 'abort' label where f54->report_size was normally zeroed out. This left f54->report_size containing its previous successful payload size. If a user then altered the V4L2 format to a smaller size, and a subsequent run failed, rmi_f54_buffer_queue() would copy the stale, larger payload size into the shrunken V4L2 buffer, causing a heap buffer overflow. Fix this by merging the 'abort' and 'error' labels into a single 'out' exit path, and ensuring that f54->report_size is always set to 0 on failure by checking for error and zeroing the local report_size first.	2026-08-26	7.8	CVE-2026-80570
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Input: byd - synchronize timer deletion before freeing private data byd_disconnect() uses timer_delete() before freeing the driver's private data. This does not wait for a running byd_clear_touch() callback, which dereferences the private data and its psmouse pointer. A callback racing with disconnect can therefore access the private data after it has been freed. The timer can also still be re-armed by byd_process_byte() while the disconnect is in progress. Use timer_shutdown_sync() before freeing the private data: it waits for a running callback and turns any later re-arm attempt into a no-op.	2026-08-26	7.8	CVE-2026-80572
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Input: cs40l50-vibra - validate custom data from user space cs40l50_add() copies the custom data of an FF_PERIODIC/FF_CUSTOM effect straight from the ff_effect the user passed to EVIOCSFF, without requiring it to hold anything: work_data.custom_data = memdup_array_user(periodic->custom_data, periodic->custom_len, sizeof(s16)); work_data.custom_len = periodic->custom_len; The driver then reads two words out of that buffer: custom_data[0] as the waveform bank in cs40l50_effect_bank_set(), and custom_data[1] as the index within the bank in cs40l50_effect_index_set(). Neither read is covered by a length check, and custom_len is fully user controlled: - custom_len == 0 makes memdup_array_user() call memdup_user() with a length of zero, which returns ZERO_SIZE_PTR rather than an error, so custom_data[0] dereferences it. - custom_len == 1 allocates two bytes. A bank of ROM or RAM keeps effect->type out of the OWT case, and custom_data[1] is then read one word past the allocation. The bank value itself is also mishandled. It is masked with CS40L50_CUSTOM_DATA_MASK (0xffff) but stored in an s16, so a custom_data[0] of 0x8000 or above wraps to a negative value that passes the "bank_type >= CS40L50_WVFRM_BANK_NUM" test. cs40l50_effect_index_set() indexes vib->dsp.banks[] with it before the switch statement's default case gets a chance to reject it: base_index = vib->dsp.banks[effect->type].base_index; max_index = vib->dsp.banks[effect->type].max_index; Require the two words the driver reads to be present, and hold the masked bank in a u32 so the existing upper-bound test covers the whole range. The da7280 haptic driver already range checks custom_len this way.	2026-08-26	7.8	CVE-2026-80575
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fbdev: core: Fix pointer desynchronization in fb_io_read() In fb_io_read(), if copy_to_user() performs a partial copy (e.g., due to a faulty user buffer), the loop adjusts the chunk size 'c' and updates the remaining 'count'. However, the hardware 'src' pointer has already been eagerly advanced by the original chunk size. If the loop is allowed to continue, the read will resume from an incorrect, over-advanced offset. Since the remaining 'count' was only decremented by the successful bytes, this desynchronization causes the next iterations to execute more hardware reads than originally bounded, eventually leading to out-of-bounds I/O reads. Fix this by breaking out of the loop immediately upon a partial copy_to_user(). A partial copy indicates a faulty user buffer, making subsequent read attempts futile. Breaking out ensures we return the number of successfully read bytes without risking out-of-bounds hardware accesses in subsequent mismatched iterations.	2026-08-26	7.3	CVE-2026-80578
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fbdev: clear fb_info->mode before deleting a videomode fb_set_var() can delete a mode from info->modelist when userspace passes FB_ACTIVATE_INV_MODE through FBIOPUT_VSCREENINFO. The code checks that the mode being deleted is not the current info->var and that fbcon is not using it, but it does not check fb_info->mode. fb_info->mode may still point into the modelist entry being deleted. If the entry is freed, later mode sysfs reads through show_mode() can dereference a	2026-08-26	7.8	CVE-2026-80579

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stale pointer. Clear fb_info->mode before calling fb_delete_videomode() when it matches the mode being removed.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fbdev: bound mode sysfs output to the sysfs buffer mode_string() uses snprintf() which can return a value larger than the remaining buffer space. show_modes() accumulates the return value into i without checking whether i has reached PAGE_SIZE, causing the offset to advance past the sysfs buffer if the modelist is long enough. Add a size parameter to mode_string() and use scnprintf() to return only the bytes actually written. Add an early return when offset already exceeds the buffer. In show_modes(), stop accumulating once the buffer is full.	2026-08-26	7.8	CVE-2026-80580
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/shmem_helper: Check VMA boundaries for PMD mappings In the ->huge_fault handler do not install a PMD huge page mapping if the huge page exceeds the boundaries of the VMA. All other ->huge_fault handlers have similar checks and the resulting mapping will trigger a VM_BUG_ON_VMA() if it ever reaches copy_pmd_range().	2026-08-26	7.8	CVE-2026-80582
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: codecs: lp-pass-tx-macro: Fix enum kcontrol accesses The "DEC0 MODE" to "DEC7 MODE" controls are enumerated, but tx_macro_dec_mode_get() and tx_macro_dec_mode_put() access their value through ucontrol->value.integer.value[0] (a long) instead of ucontrol->value.enumerated.item[0] (an unsigned int). This same pattern was fixed in the sibling drivers by commit bcf5f76cc40 ("ASoC: codecs: rx-macro: fix accessing array out of bounds for enum type") and commit 0ea5eff7c606 ("ASoC: codecs: va-macro: fix accessing array out of bounds for enum type"), but tx-macro was missed. On 64-bit kernels built with CONFIG_SND_CTL_DEBUG, the elem value sanity check catches the 4 bytes written past the enumerated item and every read of these controls fails with -EINVAL: snd-sm8250 sound: control 2:0:0:DEC0 MODE:0: access overflow	2026-08-26	7.8	CVE-2026-80583
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: reclaim forward-allocated memory on RX path errors After commit 9db5b3cec4ec ("mptcp: borrow forward memory from subflow"), errors in the receive path prior to queueing skbs into the receive queue do not trigger forward-allocated memory reclaiming. Prevent forward memory from growing unboundedly in pathological drop scenarios by explicitly reclaiming memory when skbs are dropped.	2026-08-26	7.5	CVE-2026-80588
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix listxattr handling of corrupted xattr entries Validate the xattr entry before reading its fields in f2fs_listxattr(). Return -EFSCORRUPTED when the entry is outside the valid xattr storage area instead of returning a successful partial result.	2026-08-28	7.8	CVE-2026-80591
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ntfs3: fix out-of-bounds read in decompress_lznt decompress_lznt() does not validate array index bounds before accessing the decompression table. A corrupted NTFS3 image with invalid compressed data can trigger an out-of-bounds read. Add index bounds checking to prevent the OOB access.	2026-08-28	7.8	CVE-2026-80598
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/userptr: Hold notifier_lock for write on inject test path When CONFIG_DRM_XE_USERPTR_INVAL_INJECT=y, xe_pt_svm_userptr_pre_commit() runs vma_check_userptr() with the svm notifier_lock taken for read. The test injection causes vma_check_userptr() to call xe_vma_userptr_force_invalidate(), which feeds into xe_vma_userptr_do_inval() with drm_gpumvm_ctx.in_notifier=true. That flag tells drm_gpumvm_unmap_pages() the caller already holds notifier_lock for write and only asserts the mode. Because the caller actually holds it for read, the assertion fires: WARNING: drivers/gpu/drm/drm_gpumvm.c:1669 at \drm_gpumvm_unmap_pages+0xd4/0x130 [drm_gpumvm_helper] Call Trace: xe_vma_userptr_do_inval+0x40d/0xf0 [xe] xe_vma_userptr_invalidate_pass1+0x3e6/0x8d0 [xe] xe_vma_userptr_force_invalidate+0xde/0x290 [xe] vma_check_userptr.constprop.0+0x1c6/0x220 [xe] xe_pt_svm_userptr_pre_commit+0x6a3/0xc60 [xe] ... xe_vm_bind_ioctl+0x3a0a/0x4480 [xe] Acquire notifier_lock for write in pre-commit when the inject Kconfig is enabled, via new helpers xe_pt_svm_userptr_notifier_lock()/unlock(). Rename xe_svm_assert_held_read() to xe_svm_assert_held_read_or_inject_write() so it asserts the correct mode under each build configuration. Production builds	2026-08-28	7.8	CVE-2026-80606

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CONFIG_DRM_XE_USERPTR_INVALID_INJECT=n) keep the existing read-mode behavior bit-for-bit. (cherry picked from commit 80ccbd97ffee8ad2e73167d826fe7be548364365)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: veth: fix NAPI leak in XDP enable error path During XDP enablement in veth, if xdp_rxq_info_reg() or xdp_rxq_info_reg_mem_model() fails, the driver rolls back the changes. However, the rollback loop: for (i--; i >= start; i--) { decrements the loop index 'i' before the first iteration. This correctly skips unregistering the rxq for the failed index 'i' (as registration failed or was already cleaned up), but it also erroneously skips calling netif_napi_del() for rxq[i].xdp_napi. Since netif_napi_add() was already called for index 'i', this leaves a dangling napi_struct in the device's napi_list. When the veth device is later destroyed, the freed queue memory (which contains the leaked NAPI structure) can be reused. The subsequent device teardown iterates the NAPI list and corrupts the reallocated memory, leading to UAF. Fix this by explicitly deleting the NAPI association for the failed index 'i' before rolling back the successfully configured queues.	2026-08-28	7.8	CVE-2026-80613
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: emac: Fix NULL pointer dereference in emac_probe Move devm_request_irq() after devm_platform_ioremap_resource() so that dev->emacp is mapped before the interrupt handler can fire. An early interrupt hitting emac_irq() would dereference the NULL dev->emacp and crash. Also remove redundant error message. devm_platform_ioremap_resource() already returns an error message with dev_err_probe().	2026-08-28	7.5	CVE-2026-80614
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix potential UAF in aa_replace_profiles The function aa_replace_profiles was accessing udata->size after calling aa_put_loaddata(udata), causing a potential UAF. Fixed this by saving the size to a local variable before dropping the reference.	2026-08-28	7.8	CVE-2026-80619
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: char: tlcclk: fix use-after-free in tlcclk_cleanup() This patch improves the module cleanup process in the tlcclk driver to prevent potential use-after-free and race conditions. Currently, the file_operations structure does not specify the .owner field, which could allow the module to be unloaded while user-space processes are still interacting with the device. Additionally, the tlcclk_cleanup() function frees the alarm_events memory before ensuring that blocked processes in the waitqueue are fully awakened and that the switchover_timer has completed. To address these cases, this patch: - Sets '.owner = THIS_MODULE' in tlcclk_fops to safely defer module unloading while the device is in use. - Updates tlcclk_cleanup() to explicitly wake up all blocked readers (wake_up_all), properly release hardware I/O regions, and safely delete the timer (timer_delete_sync) prior to freeing memory.	2026-08-28	7.8	CVE-2026-80622
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: seq: oss: Serialize readq reset state with q->lock snd_seq_oss_readq_clear() resets qlen, head, and tail without q->lock even though the normal reader and producer paths serialize the same ring state under that spinlock. A reset can therefore race snd_seq_oss_readq_free() or snd_seq_oss_readq_put_event() and leave stale records in the queue, drop freshly queued ones, or report the wrong readiness after wakeup. KCSAN reports a data race between snd_seq_oss_readq_clear() and snd_seq_oss_readq_free(). Take q->lock while clearing the ring and resetting input_time. Factor the enqueue logic into a caller-locked helper so snd_seq_oss_readq_put_timestamp() updates its suppression state under the same lock instead of racing the reset path. The buggy scenario involves two paths, with each column showing the order within that path: reset path: locked readq updater: 1. snd_seq_oss_reset() or 1. A reader or callback producer release reaches takes q->lock on the same queue. snd_seq_oss_readq_clear(). 2. snd_seq_oss_readq_clear() 2. The updater tests or modifies resets qlen, head, tail, qlen, head, and tail. and input_time. 3. snd_seq_oss_readq_clear() 3. The updater completes its wakes sleepers on read-modify-write sequence. q->midi_sleep. 4. Without q->lock, the reset 4. The resulting ring state drives can overlap the locked later reads and readiness. update. KCSAN reports: BUG: KCSAN: data-race in snd_seq_oss_readq_clear / snd_seq_oss_readq_free write to 0xffff8881069fe608 of 4 bytes by task 120516 on cpu 0: snd_seq_oss_readq_free+0x6c/0x80 snd_seq_oss_read+0xcb/0x250 odev_read+0x38/0x60 vfs_read+0xff/0x600 ksys_read+0xb4/0x140 __x64_sys_read+0x46/0x60 do_syscall_64+0xbb/0x2f0 entry_SYSCALL_64_after_hwframe+0x77/0x7f read to 0xffff8881069fe608 of 4 bytes by task 120517 on cpu 1: snd_seq_oss_readq_clear+0x1f/0x90 snd_seq_oss_reset+0xa7/0xf0 snd_seq_oss_ioctl+0x6f6/0x7e0	2026-08-28	7.8	CVE-2026-80628

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	odev_ioctl+0x56/0xc0 __x64_sys_ioctl+0xd1/0x120 do_syscall_64+0xbb/0x2f0 entry_SYSCALL_64_after_hwframe+0x77/0x7f value changed: 0x00000001 -> 0x00000000			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: lzo: reject compressed segment that overflows the compressed input lzo_decompress_bio() validates each on-disk segment length seg_len only against the workspace cbuf size, not against the compressed input size (compressed_len, the total folio bytes of the bio). A crafted extent can carry a segment whose seg_len passes the cbuf check but runs past the end of the bio, so copy_compressed_segment() walks off the last folio: get_current_folio() then returns the NULL folio from bio_next_folio(), and with CONFIG_BTRFS_ASSERT disabled (default) folio_size(NULL) faults. BUG: KASAN: null-ptr-deref in lzo_decompress_bio (fs/btrfs/lzo.c:383) Read of size 8 at addr 0000000000000000 by task kworker/u8:1/29 Workqueue: btrfs-endio simple_end_io_work kasan_report (mm/kasan/report.c:590) lzo_decompress_bio (fs/btrfs/lzo.c:383) end_bbio_compressed_read (fs/btrfs/compression.c:1065) btrfs_bio_end_io (fs/btrfs/bio.c:135) btrfs_check_read_bio (fs/btrfs/bio.c:180 fs/btrfs/bio.c:285) simple_end_io_work process_one_work worker_thread Reject any segment whose payload would extend beyond compressed_len before copying it, treating it as corruption like the other on-disk validation failures in this function.	2026-08-28	7.5	CVE-2026-80631
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: synproxy: fix unaligned memory access in timestamp adjustment Use get_unaligned_be32() and put_unaligned_be32() to safely read and write the timestamp fields. This prevents performance degradation due to unaligned memory access or even a crash on strict alignment architectures. This follows the implementation of timestamp parsing in the networking stack at tcp_parse_options() and synproxy_parse_options().	2026-08-28	7.5	CVE-2026-80637
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: guard against possible NULL deref in __in6_dev_stats_get() dev_get_by_index_rcu() could return NULL if the original physical device is unregistered. Found by Sashiko.	2026-08-28	7.5	CVE-2026-80646
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix OOB in scmi_power_name_get() scmi_power_name_get() does not validate the domain number passed by the external caller, which may lead to an out-of-bounds access. Fix this by returning "unknown" for invalid domains, like scmi_reset_name_get() does.	2026-08-28	7.8	CVE-2026-80649
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hfsplus: Add a sanity check for btree node size Syzbot reported an uninit-value bug in [1] with a corrupted HFS+ image, during the file system mounting process, specifically while loading the catalog, a corrupted node_size value of 1 caused the rec_off argument passed to hfs_bnode_read_u16() (within hfs_bnode_find()) to be excessively large. Consequently, the function failed to return a valid value to initialize the off variable, triggering the bug [1]. Every node starts from BTree node descriptor: struct hfs_bnode_desc. So, the size of node cannot be lesser than that. However, technical specification declares that: "The node size (which is expressed in bytes) must be power of two, from 512 through 32,768, inclusive." Add a check for btree node size base on technical specification. [1] BUG: KMSAN: uninit-value in hfsplus_bnode_find+0x141c/0x1600 fs/hfsplus/bnode.c:584 hfsplus_bnode_find+0x141c/0x1600 fs/hfsplus/bnode.c:584 hfsplus_btree_open+0x169a/0x1e40 fs/hfsplus/btree.c:382 hfsplus_fill_super+0x111f/0x2770 fs/hfsplus/super.c:553 get_tree_bdev_flags+0x6e6/0x920 fs/super.c:1694 get_tree_bdev+0x38/0x50 fs/super.c:1717 hfsplus_get_tree+0x35/0x40 fs/hfsplus/super.c:709 vfs_get_tree+0xb3/0x5d0 fs/super.c:1754 fc_mount fs/namespace.c:1193 [inline]	2026-08-28	7.8	CVE-2026-80656
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ufs: core: tracing: Do not dereference pointers in TP_printk() The trace events in drivers/ufs/core/ufs_trace.h were converted to take a pointer to the hba structure as an argument for the tracepoint and then in TP_printk() the printing of the dev_name from the ring buffer was converted to using the dev dereferenced pointer from the hba saved pointer. This is not allowed as the TP_printk() is executed at the time the trace event is read from /sys/kernel/tracing/trace file. That can happen literally, seconds, minutes, hours, weeks, days, or even months later! There is no guarantee that the hba pointer will still exist by the time it is dereferenced when the "trace" file is read. Instead, save the device name from the hba pointer at the time the tracepoint is called and place it into the ring buffer event. Then the TP_printk() can read the name directly from the ring buffer and	2026-08-28	7.8	CVE-2026-80661

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remove the possibility that it will read a freed pointer and crash the kernel. This was detected when testing the trace event code that looks for TP_printk() parameters doing illegal derferences[1] [1] https://lore.kernel.org/all/20260630184836.74d477b6@gandalf.local.home/			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: cxl: Fix CXL_HEADERLOG_SIZE to match RAS Capability size The CXL r4.0 8.2.4.17.7 RAS Capability Structure has total length 0x58 bytes (CXL_RAS_CAPABILITY_LENGTH); the Header Log occupies the trailing 64 bytes at offset 0x18. CXL_HEADERLOG_SIZE was defined as SZ_512, eight times the actual on-device size. header_log_copy() reads CXL_HEADERLOG_SIZE_U32 (128) dwords from the RAS capability iomap, overrunning the 88-byte mapping by 448 bytes. The cxl_aer_uncorrectable_error trace event memcpy()s CXL_HEADERLOG_SIZE (512) bytes from its source. For the CPER caller the source is struct cxl_ras_capability_regs::header_log[16] (64 bytes) embedded in a stack-local cxl_cper_prot_err_work_data, so the memcpy reads 448 bytes of kernel stack into the trace event ring buffer where userspace can read it via tracefs. Set CXL_HEADERLOG_SIZE to 64 and derive CXL_HEADERLOG_SIZE_U32 from it, bringing all iomap readers into agreement on 16 dwords. Userspace tools such as rasdaemon have grown a dependency on the buggy 512-byte (128 u32) header_log layout in the cxl_aer_uncorrectable_error trace event. Add CXL_HEADERLOG_TRACE_SIZE_U32 = 128 and use it for the trace event __array and its memcpy to preserve that ABI. Both callers now pass a zero-filled u32[CXL_HEADERLOG_TRACE_SIZE_U32] staging buffer with only the first CXL_HEADERLOG_SIZE_U32 (16) entries populated from hardware; the remaining 112 u32s are zero-padded, keeping the 512-byte trace ring buffer layout intact. [dj: Replaced 64 with SZ_64 per RichardC]	2026-08-28	7.1	CVE-2026-80662
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tools/power/x86/intel-speed-select: Harden daemon pidfile open Avoid symlink-based pidfile clobbering by opening the pidfile with O_NOFOLLOW and validating it with fstat() before locking/writing. The daemon currently uses a fixed pidfile path under /tmp. A local unprivileged user can pre-create a symlink at that path and cause a root-run daemon instance to write into an attacker-chosen file.	2026-08-28	7.1	CVE-2026-80663
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_nat: reject unsupported target families xt_nat SNAT and DNAT target handlers assume IP-family conntrack state is present and can dereference a NULL pointer when instantiated from an unsupported family through nft_compat. A bridge-family compat rule can therefore trigger a NULL-dereference in nf_nat_setup_info(). Reject non-IP families in xt_nat_checkentry() so unsupported targets cannot be installed. Keep NFPROTO_INET allowed for valid inet NAT compat users and leave the runtime fast path unchanged. [The crash was fixed via 9dbba7e694ec ("netfilter: nft_compat: ebttables emulation must reject non-bridge targets"), so this patch is no longer critical. Nevertheless, NAT is only relevant for ipv4/ipv6, so this extra family check is a good idea in any case.]	2026-08-28	7.3	CVE-2026-80664
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Inject SEA if kvm_translate_vncr() can't resolve PFN kvm_handle_vncr_abort() assumes that s1_walk_result conveys an abort when kvm_translate_vncr() returns -EFAULT. This is not always the case as it's possible to encounter 'late' failures on the output of S1 translation, e.g. a GFN outside of the memslots. Fix it by preparing an external abort before returning from kvm_translate_vncr(). Get rid of the BUG_ON() in the fault injection path while at it.	2026-08-28	7.1	CVE-2026-80665
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libbpf: Reject non-exclusive metadata maps in the signed loader The loader verifies map->sha against the metadata hash in its instructions. map->sha is calculated when BPF_OBJ_GET_INFO_BY_FD is called on the frozen map. While the map is frozen, the /signed loader/ must also ensure the map is exclusive, as, without exclusivity (which a hostile host could just omit when loading the loader), another BPF program with map access can mutate the contents afterwards, so the check passes on stale data. With the extra check as part of the signed loader, it now refuses to move on with map->sha validation if the host set it up wrongly.	2026-08-28	7.1	CVE-2026-80675
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: driver core: use READ_ONCE() for dev->driver in dev_has_sync_state() dev_has_sync_state() reads dev->driver twice without holding device_lock() -- once for the NULL check and once to dereference ->sync_state. Some callers only hold device_links_write_lock, which doesn't prevent a concurrent unbind from clearing dev->driver via	2026-08-28	7.8	CVE-2026-80677

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	device_unbind_cleanup(). Fix it by reading dev->driver exactly once with READ_ONCE(), pairing with the WRITE_ONCE() in device_set_driver().			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: i2c: amd-mp2: Unregister callback on adapter add failure amd_mp2_register_cb() stores the platform I2C context in the MP2 PCI driver's callback table before the adapter is registered. If i2c_add_adapter() fails, probe returns and devres frees the context, but the PCI driver can still dereference the stale pointer from its IRQ and system-sleep callbacks. Unregister the callback before returning the adapter registration error.	2026-08-28	7.8	CVE-2026-80680
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: riscv/mm: use physical alignment for vmemmap_start_pfn RISC-V computes vmemmap_start_pfn by rounding phys_ram_base down to VMEMMAP_ADDR_ALIGN. That alignment must therefore be expressed in the physical-address domain. Commit 476849b0fba4 ("riscv/mm: align vmemmap to maximal folio size") attempted to account for the maximal folio alignment by feeding MAX_FOLIO_VMEMMAP_ALIGN directly into VMEMMAP_ADDR_ALIGN. However, MAX_FOLIO_VMEMMAP_ALIGN is measured in bytes of struct page storage, whereas VMEMMAP_ADDR_ALIGN is used to align a physical address. The mask-based compound_info encoding requires pfn_to_page(0) to be naturally aligned to MAX_FOLIO_VMEMMAP_ALIGN. Commit 9f94db4c7eaa ("mm/sparse: check memmap alignment for compound_info_has_mask()") added a check for that requirement and exposed the unit mismatch on systems such as QEMU virt, where the DRAM base is not aligned to MAX_FOLIO_NR_PAGES * PAGE_SIZE. Here is the log: [0.000000][CO] -----[cut here]----- [0.000000][CO] WARNING: mm/sparse.c:365 at sparse_init+0x58a/0x6fe, CPU#0: swapper/0 [0.000000][CO] Modules linked in: [0.000000][CO] CPU: 0 UID: 0 PID: 0 Comm: swapper Not tainted 7.2.0-rc3-g1d8304bdd65f #2 PREEMPT [0.000000][CO] Hardware name: riscv-virtio,qemu (DT) [0.000000][CO] epc : sparse_init+0x58a/0x6fe [0.000000][CO] ra : sparse_init+0x58a/0x6fe [0.000000][CO] epc : ffffffff86851c88 ra : ffffffff86851c88 sp : ffffffff88807a30 [0.000000][CO] gp : ffffffff8a3bf240 tp : ffffffff88842080 t0 : ff600000fab6000 [0.000000][CO] t1 : 0000000017fab6000 t2 : 65203a6573726363 s0 : ffffffff88807bc0 [0.000000][CO] s1 : 000000000e000000 a0 : 0000000000000007 a1 : 0000000000000000 [0.000000][CO] a2 : 0000000000000002 a3 : ffffffff86851c88 a4 : 0000000000000000 [0.000000][CO] a5 : ffffffff88843080 a6 : 0000000000000003 a7 : 0000000000000000 [0.000000][CO] s2 : ff60000000000000 s3 : 0040000000000000 s4 : 0004000000000000 [0.000000][CO] s5 : ffffffff8a4d92e0 s6 : ff600000fab55e0 s7 : ffffffff88384d00 [0.000000][CO] s8 : 0000000000000003 s9 : ffffffff88384cc1 s10: ffffffff88384cc0 [0.000000][CO] s11: ffffffff8a4daae0 t3 : ffffffff915e8b20 t4 : ffffffff915e8b20 [0.000000][CO] t5 : ffffffff915e8b20 t6 : ffffffff915e8bc8 ssp : 0000000000000000 [0.000000][CO] status: 0000000200000100 badaddr: ffffffff86851c88 cause: 0000000000000003 [0.000000][CO] [<fffffff86851c88>] sparse_init+0x58a/0x6fe [0.000000][CO] [<fffffff8683d396>] mm_core_init_early+0x116/0x1e30 [0.000000][CO] [<fffffff86801edc>] start_kernel+0xd2/0x848 Convert MAX_FOLIO_VMEMMAP_ALIGN to the equivalent physical alignment before using it in VMEMMAP_ADDR_ALIGN. This keeps the existing round_down() logic while making the resulting vmemmap base satisfy the mask-alignment requirement.	2026-08-28	7.8	CVE-2026-80682
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/util: don't read __page_2 for order-1 folios in snapshot_page() snapshot_page() currently reads __page_2 after checking nr_pages > 1, but it should only do so when nr_pages > 2. If an order-1 folio is allocated at the end of a vmemmap section, __page_2 will not exist and reading it will cause a fault. During DLPAR memory remove on a 22 TB ppc64le LPAR, snapshot_page() oopsed on the page isolation path while reading an order-1 folio's __page_2 from an adjacent absent section (unmapped vmemmap). Fix this to avoid reading memmap that doesn't exist (e.g., a vmemmap hole).	2026-08-28	7.1	CVE-2026-80685
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: target: iblock: Fix wrong PR ops NULL check for PREEMPT/RELEASE In the iblock_execute_pr_out() function, PRO_PREEMPT, PRO_PREEMPT_AND_ABORT, and PRO_RELEASE all perform callback capability checks through ops->pr_clear. The error check allows unimplemented hooks to pass through the gate, resulting dereferencing a NULL function pointer. Check whether the hooks that need to be called are supported.	2026-08-28	7.5	CVE-2026-80691
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (ltc4282) Fix reading the minimum alarm voltage Coverity reports an out-of-bounds access	2026-08-28	7.8	CVE-2026-80696

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	when reading the minimum alarm voltage for the VGPIO channel. Add the missing return statement to fix the problem.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: validate external BO copy bounds for both stride paths vmw_external_bo_copy() trusts caller-supplied offsets, strides, and heights and operates on imported dma-buf vmaps: - The equal-stride memcpy() bound was clamped after subtracting the offsets from dst_size and src_size; an offset larger than the BO size wraps the unsigned subtraction to a huge value and the resulting memcpy() runs off the end of the vmap. dst_stride * height is also a u32 multiplication that can overflow. - The non-equal-stride row-by-row path had no bound at all. The loop touches bytes through offset + (height - 1) * stride + width_in_bytes, with only a WARN_ON(dst_stride < width_in_bytes), and could likewise step past the end of either mapping. The offsets and strides are derived from STDU/SOU plane state, so a configured CRTC submitting a crafted atomic commit on an imported framebuffer can reach this path. Validate the exact row-copy endpoint against each BO's size up front using check_mul_overflow() and check_add_overflow(). Use the bulk memcpy() path only when width_in_bytes covers the whole stride; otherwise copy one row at a time so partial-row updates near the bottom of a framebuffer remain valid. Also reject zero strides and stride < width_in_bytes, both of which the row-by-row path cannot represent safely.	2026-08-28	7.8	CVE-2026-80700
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: fix guest_memory_dirty bitfield clobbered as size Two sites in vmwgfx_resource.c assign boolean literals to res->guest_memory_size, which is an unsigned long allocation-size field; the intended target is the adjacent res->guest_memory_dirty bitfield. After the assignments the field holds 0 or 1 instead of the resource's MOB allocation size: - vmw_resource_release() writes 0 (false), and - vmw_resource_unbind_list() writes 1 (true). Subsequent revalidation paths read guest_memory_size when computing the dirty page range (vmw_bo_dirty_transfer_to_res()) and the buffer allocation size (vmw_resource_buf_alloc()), producing zero-length walks or wrap-around ranges that read or write past the MOB bitmap. The dirty-tracking intent of the original code (mark the resource as dirtied since the last sync) is also lost, since guest_memory_dirty is never updated. Rename both assignments to guest_memory_dirty.	2026-08-28	7.8	CVE-2026-80702
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: softing: fw_parse(): validate firmware record spans fw_parse() reads a fixed record header, a firmware-provided payload, and a trailing checksum without knowing the end of the firmware blob. A truncated record can therefore make those reads exceed the blob. The same record also supplies addresses and lengths for writes into DPRAM. The generic loader uses wrap-prone mixed signed arithmetic for its bounds check, while the application loader does not bound the staging copy at all. Pass the firmware end to the parser and validate the full source record. Use a signed wide offset for generic DPRAM records and validate the application staging span against the mapped DPRAM before copying.	2026-08-28	7.8	CVE-2026-80706
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: can: j1939: transport: j1939_session_fresh_new(): initialize receive buffer Zero the allocated buffer in j1939_session_fresh_new() to ensure it contains no residual data. While there is a potential performance impact if users allocate maximum sized ETP buffers, most real-world use cases are not noticeably affected since the maximum known buffer size is typically around 65K. [mkl: add Message-ID]	2026-08-28	7.5	CVE-2026-80707
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: Fix wrong domain value verification with EP11 CPRBs There is a wrong upper limit check for the domain value when an EP11 CPRB is processed for sending to a crypto card. This check is only active on custom device nodes but may lead to access heap memory behind perms->adm when an administrative CPRB is sent. Add correct limit (AP_DOMAINS = 256) checking to fix this.	2026-08-28	7.8	CVE-2026-80709
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: Fix undersized format-check buffer fmt_buffer_size in dasd_eckd_check_device_format() is declared as int, even though one of the multiplicands, sizeof(struct eckd_count), is a size_t. The expression trkcount * rpt_max * sizeof(struct eckd_count) is therefore correctly evaluated at 64-bit width, but the result is silently truncated when it is stored back into the 32-bit fmt_buffer_size variable. For a sufficiently large track range (start_unit/stop_unit are caller-controlled) this truncation yields a buffer size far smaller than the	2026-08-28	7.8	CVE-2026-80710

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	number of tracks actually requested. kcalloc() then succeeds with an undersized allocation, while the subsequent channel program build still operates on the untruncated track count and writes past the end of that buffer. Compute the buffer size with check_mul_overflow() and keep it in a size_t, so that a value that no longer fits results in -EINVAL instead of a silently truncated allocation size.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: wake linked drain waiters on unlink snd_pcm_drain() on a linked stream parks an on-stack wait entry on the drained peer's runtime->sleep, and after schedule_timeout() removes it only if that peer is still found in the caller's group. If group membership changes during the wait and the sleep ends by signal or timeout (so autoremove_wake_function() does not run), finish_wait() is skipped and snd_pcm_drain() returns with the entry still queued on that stream's sleep list; a later wake_up() then walks a freed stack frame. This is reachable by unlinking either the drained or the draining stream. Unlike the close path (snd_pcm_drop() -> snd_pcm_post_stop()), snd_pcm_unlink() never wakes the sleep queues. Wake every group member under the group lock before the membership change, so a linked drainer is released and drops its entry while the streams are still grouped. The window was opened when snd_pcm_link_rwsem stopped being held across the wait and the removal became conditional on group membership (see Fixes). The later switch to finish_wait() kept that conditional removal, so the signal/timeout case remained.	2026-08-28	7.8	CVE-2026-80716
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: validate Adaptation Indication parameter length The Adaptation Layer Indication parameter contains a fixed 32-bit Adaptation Code Point after its parameter header. However, sctp_verify_param() accepts a header-only parameter because the generic parameter walker only requires the header to be present. sctp_process_param() then reads adaptation_ind beyond the declared parameter. When the malformed parameter is last in an INIT, the read starts at the receive skb tail, and the value is copied into the state cookie returned in the INIT ACK. This may disclose four receive-buffer tail bytes. Require the declared parameter length to match the fixed structure size and abort the association through the existing invalid parameter length path otherwise.	2026-08-28	7.5	CVE-2026-80717
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/percpu-km: fix bitmap overflow and accounting in pcpu_create_chunk() In pcpu_create_chunk(), nr_pages is the total contiguous backing allocation, i.e., nr_units * pcpu_unit_pages, but pcpu_chunk_populated() uses it to set chunk->populated, whose size is pcpu_unit_pages, bitmap. Since bit N in chunk->populated means page offset N inside every unit is backed. When nr_units > 1, the function writes beyond chunk->populated. Fix it by using chunk->nr_pages. It also fixes the global pcpu_nr_empty_pop_pages accounting, since pcpu_balance_free() only iterates up to chunk->nr_pages. Commit a63d4ac4ab609 ("percpu: make percpu-km set chunk->populated bitmap properly") introduced the bitmap overflow issue. Later, commit b539b87fed37f ("percpu: implemeent pcpu_nr_empty_pop_pages and chunk->nr_populated") added pcpu_nr_empty_pop_pages and caused the accounting issue.	2026-08-28	7.8	CVE-2026-80718
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iomap: add a separate bio_set for iomap_split_ioend iomap_split_ioend can split bios that already come from iomap_ioend_bioset and thus deadlock when the bioset is exhausted. Add a separate bio_set to avoid this deadlock. Christian Brauner <brauner@kernel.org> says: Mark iomap_ioend_split_bioset static as it is only used in ioend.c, fixing the sparse warning reported by the kernel test robot.	2026-08-28	7.5	CVE-2026-80720
Liquid Web / StellarWP--GiveWP	Deserialization of Untrusted Data vulnerability in Liquid Web / StellarWP GiveWP allows Object Injection. This issue affects GiveWP: from n/a through 4.16.7.1.	2026-08-28	10	CVE-2026-82222
Liquid Web / StellarWP--WPComplete	Unauthenticated Cross Site Scripting (XSS) in WPComplete <= 2.9.5.6 versions.	2026-08-24	7.1	CVE-2026-66599
Liquid Web, LLC--Kadence Shop Kit	Subscriber SQL Injection in Kadence Shop Kit <= 3.0.6 versions.	2026-08-27	8.5	CVE-2026-32550
LiquidThemes--Booking Hub	Subscriber Privilege Escalation in Booking Hub <= 1.3.0 versions.	2026-08-24	8.8	CVE-2026-32561
LiquidThemes--MagicAI for WordPress - AI Text, Image, Chat,	Subscriber Local File Inclusion in MagicAI for WordPress - AI Text, Image, Chat,	2026-08-24	8.8	CVE-2026-32560

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Code, and Voice Generator				
litespeedtech--LiteSpeed Cache	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Comment Content in all versions up to, and including, 7.8.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. A comment payload crafted exclusively from decimal numeric character references (e.g. ", <, >) placed inside an allowed element such as <code> bypasses WordPress's wp_kses sanitization, as kses does not treat a data-settings="..." substring within text content as an HTML attribute, allowing the malicious payload to reach the vulnerable function. For this to be exploitable, the site must allow users with previously approved comments to write new comments, and the require_name_email setting must be disabled.	2026-08-28	7.2	CVE-2026-18978
LoftOcean--CozyStay	Unauthenticated Cross Site Scripting (XSS) in CozyStay <= 1.10.0 versions.	2026-08-27	7.1	CVE-2026-78289
MacWarrior--clipbucket-v5	ClipBucket V5's web installer fails to properly validate or escape the php_cli_filepath parameter before passing it to shell execution. Unauthenticated attackers can submit a crafted POST request to the installer with a malicious php_cli_filepath value to execute arbitrary commands as the web server user.	2026-08-25	9.8	CVE-2026-80138
magepeopleteam--Booking and Rental Manager	Contributor PHP Object Injection in Booking and Rental Manager <= 2.7.5 versions.	2026-08-27	8.8	CVE-2026-78257
mapfish--mapfish-print	mapfish-print is a component of MapFish for printing templated cartographic maps. Prior to 3.28.30, 3.30.32, 3.31.24, 3.33.16, and 4.0.5, MapFish Print accepts an attacker-controlled GML layer url in requests to the /api/print3/print endpoint and fetches XML parsed by core/src/main/java/org/mapfish/print/map/geotools/GmlLayer.java without disabling external entities and external DTDs. A remote XML document and DTD can expand a local file entity, and the resulting content can be exposed through the GML parsing and error path. This allows unauthenticated attackers to read files such as operating-system account data, Kubernetes service-account tokens, and certificates. Replacing the file entity target with an internal HTTP endpoint also permits server-side request forgery. This issue is fixed in versions 3.28.30, 3.30.32, 3.31.24, 3.33.16, and 4.0.5.	2026-08-28	8.6	CVE-2026-55848
maquina-app--rails-mcp-server	The execute_ruby tool is documented as a read-only Ruby sandbox and is enforced by a pattern denylist together with replacements for the process-spawning methods on Kernel. The pseudo-terminal library's spawn entry points are neither in the denylist nor replaced, so a normal tool call could reach them and start a shell, executing commands as the account running the server and outside the guarded methods. The denylist was introduced with the tool in 1.4.0 and never covered those entry points through 1.6.0. Version 1.6.1 restricts the requires the sandbox permits to a data-only list and blocks dynamic dispatch to execution entry points; 2.0.0 removes the tool.	2026-08-27	8.4	CVE-2026-81097
mariadb-corporation--mariadb-connector-nodejs	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. Prior to versions 3.3.3, 3.4.6, and 3.5.3, when ssl is enabled without a pinned CA or server certificate, MariaDB Connector/Node.js sends credentials before completing certificate fingerprint validation. In lib/cmd/handshake/auth/handshake.js, a server that selects mysql_clear_password as the initial authentication plugin can receive the password before the post-TLS identity check. In lib/cmd/handshake/authentication.js, an authentication switch can evaluate the previous plugin instead of the requested target plugin, allowing mysql_clear_password to send the credential first. An active man-in-the-middle can present a self-signed certificate, capture the database password, and use it to authenticate directly even though the connector later rejects the server and closes the connection. This issue is fixed in versions 3.3.3, 3.4.6, and 3.5.3.	2026-08-28	7.5	CVE-2026-55215
mcp-router--mcp-router	The mcp-router CLI served its MCP aggregator on every interface and enforced authentication only when the operator asked for it. The serve command in apps/cli/src/commands/serve.ts defaulted its host to the all-interfaces address on a fixed port, and required a token only when the corresponding flag was supplied, so a default invocation exposed the aggregator, and every MCP server it fronted, to anyone able to reach the port. Release 0.6.3 defaults the host to the loopback	2026-08-27	9.1	CVE-2026-81094

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	address and refuses to start without a token whenever the host it is given is not a loopback address; no earlier release carries either check.			
mcp-use--mcp-use	The proxy middleware in mcp-use's inspector forwards requests to a destination the caller names. mountMcpProxy in libraries/typescript/packages/inspector/src/server/proxy/mcp-proxy.ts read the target from the X-Target-URL header or the __mcp_target parameter and proxied to it without inspecting the host, so loopback, link-local and private addresses were all accepted, as were names that resolve to them, and the validation was not reapplied to a redirect the destination returned. A caller could therefore make the server issue requests to addresses reachable only from the host it runs on and read the responses. The current code calls isSafeProxyTarget, which checks the resolved address against private, loopback and link-local ranges before proxying and bounds the number of redirects followed.	2026-08-27	8.6	CVE-2026-81091
melograno--Booking for Appointments and Events Calendar Amelia	The Booking for Appointments and Events Calendar - Amelia plugin for WordPress is vulnerable to Stored Cross-Site Scripting via customer name fields in versions up to and including 2.2. This is due to an authentication bypass where the AddBookingCommand explicitly skips nonce verification (Command.php line 186), allowing unauthenticated users to submit booking data. While the plugin applies sanitize_text_field() to customer firstName and lastName fields (BookingApplicationService.php lines 302-308), this function only removes HTML tags and preserves special characters including double quotes. The vulnerability manifests in the administrative Calendar view where a FullCalendar eventContent callback interpolates customer names directly into JavaScript template literals (redesign/dist/index.js line 199) and renders them via innerHTML without proper HTML entity encoding. Because double quotes are preserved, an attacker can inject payloads like "" onmouseover=""alert(document.cookie)"" to break out of the title attribute and inject malicious event handlers. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute when an administrator accesses the Calendar page and hovers over the malicious appointment.	2026-08-28	7.2	CVE-2026-6286
mercadopago--mercadopago	The Mercado Pago Node.js SDK interpolates caller-supplied identifiers into API request paths without percent-encoding them, so characters that are structural in a URL survive into the outgoing request. The payment (get, capture, cancel), paymentRefund (create, total, list, get), advancedPayment (get, capture, cancel, update, updateReleaseDate) and disbursementRefund (create, createAll, listAll) clients build their path as a template literal, for example RestClient.fetch(`/v1/payments/\${id}`, ...) in src/clients/payment/get/index.ts. A dot-dot or slash sequence in the identifier is normalised by the WHATWG URL parser and redirects the request to a different endpoint, and a question mark appends attacker-chosen query parameters, in both cases carrying the merchant's own access token. An application that forwards an identifier influenced by an untrusted party into one of these methods without an ownership check therefore allows that party to reach other resources within the merchant's token scope. The repository already contains the intended helper, encodePathParam in src/utlis/path.ts, which pull request 451 applied to roughly 29 other clients while leaving these unchanged.	2026-08-24	8.2	CVE-2026-76842
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.58, Browser Server _handle_connection() checks Chrome extension origins with re.match() and the unanchored expression chrome-extension://[a-z0-9]{32}. Extra trailing characters pass before websocket.accept(), allowing start_session commands and unauthorized browser automation. This issue is fixed in version 4.6.58.	2026-08-25	9.1	CVE-2026-55536
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonaiagents 1.6.58, spider_tools._host_is_blocked() does not resolve ordinary hostnames before scrape_page fetches them. A hostname such as 127.0.0.1.nip.io passes validation and resolves to loopback, permitting internal HTTP access. The fix uses socket.getaddrinfo and fails closed on DNS errors. This issue is fixed in version 1.6.58.	2026-08-25	8.5	CVE-2026-55526
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonaiagents 1.6.58, AgentServer exposes ServerConfig.auth_token but AgentServer._create_app does not check it on any route. A remote caller can subscribe, publish, and perform other actions without a valid bearer token or X-Auth-Token even when authentication is configured. This issue is fixed in version 1.6.58.	2026-08-25	8.2	CVE-2026-55528
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.58, create_auth_middleware() allows requests when auth=api-key lacks	2026-08-25	8.2	CVE-2026-55533

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	PRAISONAI_API_KEY or JWT authentication lacks PRAISONAI_JWT_SECRET. An externally bound Recipe server can therefore accept unauthenticated POST /v1/recipes/run requests despite authentication being enabled. This issue is fixed in version 4.6.58.			
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. From praisonai 4.6.34 until 4.6.58, praisonai serve agents accepts --api-key but _create_agents_app() does not authenticate POST /agents or POST /agents/{agent_name}. A network caller can invoke configured agents without credentials even when an API key was supplied. This issue is fixed in version 4.6.58.	2026-08-25	8.6	CVE-2026-55534
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.51, the Jobs API create_app function mounts /api/v1/runs without authentication. Any reachable caller can submit jobs, read results, cancel runs, or delete jobs using operator credentials. The fix adds PRAISONAI_JOBS_API_KEY middleware for Authorization or X-API-Key. This issue is fixed in version 4.6.58.	2026-08-25	8.6	CVE-2026-55539
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonaiagents 1.6.58, the web_crawl function validates only the initial URL before _crawl_with_httpx uses httpx.Client(follow_redirects=True). Redirect targets are not revalidated, so an attacker who influences a crawl target can redirect a public URL to loopback, private network, or cloud metadata services while ALLOW_LOCAL_CRAWL remains disabled. The fetched internal response is returned to the agent context. This issue is fixed in version 1.6.58.	2026-08-25	7.5	CVE-2026-55525
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonaiagents 1.6.58, the FileMemory constructor joins unsanitized user_id into self.user_path. A caller supplying ../ or path separators can escape the memory directory and write JSON data to arbitrary process-writable locations. The fix sanitizes user_id before constructing self.user_path. This issue is fixed in version 1.6.58.	2026-08-25	7.1	CVE-2026-55527
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.58, MCP HTTP Stream _validate_origin uses request_origin.startswith(allowed), allowing the attacker-controlled localhost.attacker.com HTTP origin to satisfy the localhost allowlist. A webpage can send Content-Type: text/plain requests without preflight and invoke tools/call without an API key, including file writes that persist agent instructions. This issue is fixed in version 4.6.58.	2026-08-25	7.6	CVE-2026-55532
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.58, JobSubmitRequest.validate_webhook_url() accepts webhook_url when resolution raises socket.gaierror because the exception path uses except socket.gaierror: pass. JobExecutor._send_webhook() later performs a fresh lookup, allowing DNS changes to direct the request to an internal service. This issue is fixed in version 4.6.58.	2026-08-25	7.1	CVE-2026-55537
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.51, praisonai serve agents parses config["api_key"] but _create_agents_app() does not authenticate POST /agents or POST /agents/{agent_name}. Missing or incorrect bearer and X-API-Key values still reach agent execution. This issue is fixed in version 4.6.58.	2026-08-25	7.3	CVE-2026-55538
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.51, is_path_within_directory() uses os.path.abspath() rather than os.path.realpath() for the workspace boundary. A symlink inside workspace can point outside and still pass the check, allowing read_file and other code tools to access files outside the configured workspace. This issue is fixed in version 4.6.58.	2026-08-25	7.1	CVE-2026-55540
Microsoft--Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-08-28	8.8	CVE-2026-72984
midday-ai--midday	Midday allows any member of a team to delete it. The delete procedure in apps/api/src/trpc/routers/team.ts authorises the caller with the team-access helper, which returns true for every row in the team-membership table irrespective of the role it records, and the data-layer function it calls re-checks the same helper and nothing else. The neighbouring procedures that remove or update a member in the same router each resolve the caller's role and refuse the request unless it is owner, so the check exists in the file and is not applied to deletion. Member is the role an invited user receives, so any invitee can remove the team and every record scoped to it, and the deletion enqueues the cleanup job with the stored bank-connection tokens, which the job then uses against the connected providers. The update procedure in the same router carries no role check either.	2026-08-26	8.1	CVE-2026-81035
Mikado-Themes--Verdure Core	The Verdure Core plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.2. This makes it possible for unauthenticated attackers to include and execute arbitrary files on the server, allowing the	2026-08-25	8.1	CVE-2026-78562

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other "safe" file types can be uploaded and included.			
Milesight--AM102/102L V2	A cleartext transmission of sensitive information vulnerability in the NFC interface of multiple Milesight IoT device models running affected firmware versions allows an unauthenticated attacker with physical proximity to retrieve LoRaWAN ABP NwkSKey and AppSKey values and D2D keys via an NFC read operation. The exposed keys can be used to decrypt LoRaWAN traffic, forge uplink and downlink frames, submit falsified sensor data, issue supported device commands, and cause subsequent legitimate frames to be rejected.	2026-08-26	7.6	CVE-2026-29988
mims-harvard--ToolUniverse	ToolUniverse ran caller-supplied Python inside a sandbox that could be escaped, on a server that required no authentication. The executor behind the python_code_executor tool, in python_executor_tool.py, inspected the submitted source for a denied list of attribute names and calls but left the attribute-lookup builtins available and did not stop a dunder attribute reached through a string lookup or through a module already permitted, so a caller could walk from a literal's class to its base and enumerate subclasses to obtain a reference to the process and subprocess modules. A per-call argument also let the caller widen the import allow-list before the inspection ran. The HTTP and MCP servers in http_api_server.py and smcp_server.py bound to every interface with debugging enabled and no authentication, so any caller able to reach the port executed code as the server process. Version 1.3.0 adds bearer-token authentication, defaults the bind address to loopback, and hardens the attribute checks.	2026-08-27	10	CVE-2026-81096
MongoDB--BI Connector	In MongoDB Connector for BI, MongoDB object names such as collection, field, and index names are placed into the quoted identifiers of the DDL text returned by SHOW CREATE statements without escaping the identifier delimiter. A user with permission to write to a sampled MongoDB collection can choose a name that closes the quoted identifier early, so that additional SQL text becomes part of the generated output. If an operator or automated tool later replays that generated statement against a SQL server, the additional text is executed with the privileges of that session.	2026-08-28	8	CVE-2026-77586
MongoDB--BI Connector	A database user able to create a view in a namespace that MongoDB Connector for BI samples can cause the schema-sampling routine to stop functioning by defining a view whose evaluation reliably fails. The sampling logic classifies the resulting server message as transient and, after the configured retries are exhausted, proceeds without a valid result, ending the schema refresh routine. The mongosqld process continues running without a usable schema, so SQL clients are unable to obtain results until an operator removes the view or excludes its namespace from sampling.	2026-08-28	7.7	CVE-2026-81490
MongoDB--BI Connector	An unauthenticated party able to reach the port of a MongoDB Connector for BI (mongosqld) instance may generate enough routine connection log activity to exhaust the storage backing the configured log path. When a log write or log rotation operation subsequently fails, the resulting error is not handled and the shared mongosqld process ends, ending service for all connected SQL clients. The process continues to end on startup until an operator restores available storage, and the diagnostic message explaining the condition is not recorded.	2026-08-28	7.5	CVE-2026-81517
MongoDB--BI Connector	When mongosqld is configured with a client certificate authority file, the listener requests a client certificate during the TLS handshake but does not require one, so a client that presents no certificate is still accepted. In deployments that rely on client certificates as the sole means of identifying users, a remote party with network access to the listener can therefore establish a session and read the MongoDB data exposed through the connector.	2026-08-28	7.5	CVE-2026-81518
MongoDB--BI Connector	A network-reachable client that has not yet authenticated can hold a MongoDB Connector for BI authentication session open indefinitely by beginning a SASL-based login exchange and then declining to complete it. Because the negotiation loop had no overall time bound and the read from the client had no deadline, each such session retains a worker, a client connection slot, and its associated backend database connections until the process is restarted. Repeated use of this behavior can consume the configured connection capacity and prevent legitimate users from establishing new sessions.	2026-08-28	7.5	CVE-2026-81520
MongoDB--BI Connector ODBC Driver	A user able to submit SQL through an application using the MongoDB Connector for BI ODBC driver can supply a positioned-cursor statement whose cursor name exceeds the size of an internal fixed-length buffer. Because the name length is not bounded before the driver builds its diagnostic message, memory adjacent to that	2026-08-28	8.8	CVE-2026-81532

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	buffer is overwritten with user-supplied content. This can terminate the hosting application process and may allow unintended code to run within it.			
MongoDB--BI Connector ODBC Driver	An application using the MongoDB BI Connector ODBC Driver may encounter a memory-safety issue when a submitted SQL statement contains an unusually long run of digits following a LIMIT clause. The issue occurs only on connections where the driver's optional prefetch setting is enabled, and stems from the driver copying the digit sequence into a fixed-size internal buffer without checking its length. A user able to influence the numeric portion of a LIMIT clause could cause the hosting application process to terminate unexpectedly or corrupt adjacent memory in that process.	2026-08-28	7.1	CVE-2026-81533
MongoDB--C# Driver	Improper neutralization of delimiters in connection-URL construction allows connection-option injection in the MongoDB C# Driver. When an application passes untrusted text into the driver's connection-URL builder and round-trips the builder back into a client configuration, the untrusted text is serialized without neutralizing the URL/option delimiters and is then re-parsed as authoritative connection options. A low-privileged user of such an application can thereby introduce or suppress security-relevant connection settings.	2026-08-27	7.1	CVE-2026-81529
MongoDB--C++ Driver	A weakness in the MongoDB C++ Driver's handling of caller-supplied namespace identifiers allows special characters embedded in those identifiers. An application that builds a namespace identifier from untrusted input without validating it may therefore have its operation directed at a different target than intended. This can result in limited unauthorized read and write access to data belonging to another logical tenant of the affected application.	2026-08-27	8.1	CVE-2026-81522
MongoDB--PHP Library	The MongoDB client library for PHP does not sufficiently sanitize special elements in application-supplied namespace identifiers before using them to construct the target namespace for database operations. An application that incorporates untrusted text into these identifiers may have operations silently directed at a different storage location than the one the application intended.	2026-08-27	8.1	CVE-2026-81525
mra13--Stripe Payments	Unauthenticated Cross Site Scripting (XSS) in Stripe Payments <= 2.1.2 versions.	2026-08-24	7.1	CVE-2026-78282
multer--multer	multer is a middleware for handling multipart/form-data in Node.js. In version 2.2.0, when a disk-backed upload is aborted or truncated before the write stream finishes, multer's disk storage engine removes the visible file but does not close the underlying write file descriptor, leaving a deleted but still open descriptor. A remote attacker able to reach an upload route using the built-in disk storage can send repeated aborted or malformed multipart uploads, each one leaking a file descriptor and retaining disk blocks until the process exits, which can exhaust resources and cause a denial of service. The issue is fixed in multer 2.3.0, which closes the destination write stream on abnormal source termination and defers cleanup until the stream has closed. Upgrade to multer 2.3.0 to remediate.	2026-08-28	7.5	CVE-2026-77037
multer--multer	multer is a middleware for handling multipart/form-data in Node.js. A small multipart request containing two specially crafted text field names can cause an uncaught RangeError (Invalid array length) that terminates the Node.js process. The first field uses a very large numeric array index to allocate a maximum-length sparse array, and a second field then pushes past that length, which throws inside the append-field dependency and is not caught by multer. All versions before 2.3.0 are affected, and the issue is a remotely triggerable denial of service. The issue is fixed in multer 2.3.0. Upgrade to multer 2.3.0 to remediate.	2026-08-28	7.5	CVE-2026-77078
multer--multer	multer is a middleware for handling multipart/form-data in Node.js. A small multipart request with two specially crafted text field names can make multer's field parser synchronously iterate a maximum-length sparse array, blocking the event loop so the process cannot handle other requests. A large numeric array index in the first field allocates a maximum-length sparse array, and a second field with a non-numeric key then triggers a full-length iteration inside the append-field dependency. All versions before 2.3.0 are affected, and this is a remotely triggerable denial of service. multer 2.3.0 adds an opt-in fieldArrayIndexLimit option that rejects oversized array indexes. Upgrade to multer 2.3.0 and set limits.fieldArrayIndexLimit to the largest array index your application needs to remediate.	2026-08-28	7.5	CVE-2026-82333
MVPThemes--Jawn	Unauthenticated Privilege Escalation in Jawn <= 1.4.2 versions.	2026-08-24	9.8	CVE-2026-66648
MVPThemes--Jawn	The Jawn theme for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.4.2. This makes it possible for unauthenticated attackers to elevate their privileges to that of an administrator.	2026-08-25	9.8	CVE-2026-78477

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NASA--cFS	A security flaw has been discovered in NASA cFS up to 7.0.1. The affected element is the function CFE_SB_GetUserDataLength of the file src/cfs/cfe/modules/sb/fsw/src/cfe_sb_util.c of the component cFE Software Bus. Performing a manipulation of the argument TotalMsgSize/HdrSize results in integer underflow. It is possible to initiate the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-30	7.4	CVE-2026-82480
NASA--Trick	A vulnerability was determined in NASA Trick 19.6.0. This issue affects the function JSONVariableServerThread::parse_request of the file trick_source/sim_services/JSONVariableServer/JSONVariableServerThread.cpp of the component TCP Socket Handler. This manipulation causes stack-based buffer overflow. The attack is possible to be carried out remotely. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-30	7.3	CVE-2026-82478
ncopa--su-exec	su-exec through 0.3 fails to validate numeric user and group identifiers parsed with strtol before assigning to uid_t and gid_t, allowing truncation of out-of-range values to zero. Attackers can supply large numeric identifiers that truncate to root's identifier, causing su-exec to execute target programs with root privileges instead of intended unprivileged accounts.	2026-08-29	7.8	CVE-2026-82457
nektos--act	act starts an HTTP Artifacts V4 backend whenever a workflow uses actions/upload-artifact@v4 or actions/download-artifact@v4. The control-plane RPCs of that backend, including CreateArtifact, GetSignedArtifactURL, ListArtifacts, FinalizeArtifact and DeleteArtifact, accept a caller-supplied workflow_run_backend_id and never check that it belongs to the requester: validateRunIDV4 in pkg/artifacts/artifacts_v4.go parses the value and returns it with the comparison against the requesting task's run ID left commented out. The signed URLs the backend issues are authenticated by an HMAC whose key is hardcoded to the four bytes 0xba 0xdb 0xee 0xf0, identical in every build, computed over a concatenation of endpoint, expiry, artifact name and task ID with no length prefix or delimiter, so signatures are both forgeable and ambiguous between differing artifact name and task ID pairs. The --artifact-server-addr flag defaults to the host's outbound address rather than loopback, leaving the backend reachable from the surrounding network. Any client that can reach it may read, overwrite or delete the artifacts of a concurrently running job with no credentials, exposing build outputs such as secrets and deployment credentials and permitting their replacement before the owning job consumes them.	2026-08-24	8.8	CVE-2026-76847
Netis Systems--NC63	Netis NC63 firmware through V3.0.0.3327 contains a stack-based buffer overflow vulnerability that allows unauthenticated remote attackers to overwrite saved stack state by submitting an oversized Base64-encoded password to the login handler in /bin/netis.cgi. Attackers can exploit the custom Base64 decoder's lack of output length validation against the fixed-size stack buffer to achieve remote code execution with root privileges, as the Boa web server executes the CGI environment as root.	2026-08-24	9.8	CVE-2026-76070
Netis Systems--NC63	Netis NC63 firmware through V3.0.0.3327 contains a stack-based buffer overflow vulnerability that allows unauthenticated remote attackers to overwrite saved stack state by supplying an oversized destHost parameter to the ipFilterList=mod action in netis.cgi. Attackers can exploit widthless sscanf conversions that copy user-supplied input into fixed-size stack buffers before authentication is verified, achieving remote code execution as root due to the Boa web server executing the CGI environment with root privileges.	2026-08-24	9.8	CVE-2026-76071
Network Optix--Nx Witness VMS	Cross-site scripting in the Web Administration interface of Network Optix Nx Witness VMS before version 6.1.3 on Linux, Windows and MacOS allows an adjacent-network attacker to execute arbitrary JavaScript in the browser of an authenticated administrator and steal the administrator's session token, resulting in Administrator Account Takeover. An attacker who controls an Nx server on the same network segment can set that server's site name to a script payload, which executes when an administrator opens the "Merge with Another Site" dialog and the site selection list is displayed.Solution: Update to Nx Witness VMS version 6.1.3 or later.	2026-08-24	8	CVE-2026-78414
Nexcess--Event Tickets	Unauthenticated Cross Site Scripting (XSS) in Event Tickets <= 5.29.2.1 versions.	2026-08-24	7.1	CVE-2026-78263
Nexcess--The Events Calendar	Unauthenticated PHP Object Injection in The Events Calendar <= 6.17.2 versions.	2026-08-24	9.8	CVE-2026-78265
nfriedly--bestzip	bestzip builds the argument list for the system zip utility without separating options from operands. The destination archive path and the caller-supplied source paths are passed to the child process with no -- delimiter between them, so any	2026-08-26	8.4	CVE-2026-80427

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	source entry beginning with a hyphen is interpreted by zip as an option rather than a file name. zip accepts -T to test the finished archive and -TT to name the command used to perform that test, so a source list containing those two entries and a command string causes zip to run that command through a shell once the archive has been written. An application that passes a file name or path it received from an untrusted source into the bestzip API therefore executes a command of the supplier's choosing. Versions 2.2.6 and 3.0.2 add the delimiter.			
NI--LabVIEW	There is a memory corruption vulnerability recently discovered in NI LabVIEW that may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2026 Q3 (26.3.0) and prior versions.	2026-08-25	7.8	CVE-2026-16233
NI--LabVIEW	There is a memory corruption vulnerability recently discovered in NI LabVIEW that may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2026 Q3 (26.3.0) and prior versions.	2026-08-25	7.8	CVE-2026-16234
NI--LabVIEW	There is a memory corruption vulnerability recently discovered in NI LabVIEW that may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2026 Q3 (26.3.0) and prior versions.	2026-08-25	7.8	CVE-2026-64201
NI--LabVIEW	There is a memory corruption vulnerability recently discovered in NI LabVIEW that may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2026 Q3 (26.3.0) and prior versions.	2026-08-25	7.8	CVE-2026-64202
NI--LabVIEW	There is a memory corruption vulnerability recently discovered in NI LabVIEW that may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2026 Q3 (26.3.0) and prior versions.	2026-08-25	7.8	CVE-2026-64203
NI--LabVIEW	There is a memory corruption vulnerability recently discovered in NI LabVIEW that may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI. This vulnerability affects NI LabVIEW 2026 Q3 (26.3.0) and prior versions.	2026-08-25	7.8	CVE-2026-64204
nimiq--core-rs-albatross	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Through 1.5.0, the validity store uses a strict lower-bound comparison that expires a stored transaction too early relative to Transaction::is_valid_at, allowing a remote attacker to replay the same signed transaction during a blocks_per_batch minus one block window and cause the sender and recipient balances to be updated twice. This issue is fixed in version 1.5.1.	2026-08-26	7.5	CVE-2026-46369
nlTK--nlTK	NLTK before 3.10.0 (affected versions <=3.9.4) contains an unsafe pickle deserialization vulnerability in the TransitionParser.parse() method (nlTK/parse/transitionparser.py). The method calls pickle_load() with the default restricted=False, routing deserialization through WarningUnpickler, which does not override find_class() and therefore permits arbitrary class resolution. When an application loads an attacker-crafted model file, embedded pickle gadget chains execute arbitrary Python code with the privileges of the user running the application. NLTK provides a RestrictedUnpickler for safe deserialization, but it is not used by production code paths. Fixed in 3.10.0.	2026-08-25	9.6	CVE-2026-78683
nlTK--nlTK	NLTK versions before 3.10.3 contain a remote code execution vulnerability in allowlisted pickle loaders that trust entire module namespaces instead of specific safe callables. Attackers can craft malicious pickle payloads invoking dangerous in-namespace functions like ReppTokenizer._execute and numpy.f2py.crackfortran.myeval through pickle REDUCE to execute arbitrary commands during model or tokenizer artifact loading.	2026-08-25	9.8	CVE-2026-79657
nlTK--nlTK	NLTK before 3.10.3 fails to validate JVM options passed through the per-call options parameter in the java() function, allowing attackers to inject dangerous JVM flags. Attackers can supply malicious options like -agentpath, -javaagent, or @argfile to Stanford wrapper classes to achieve arbitrary code execution.	2026-08-25	9.8	CVE-2026-79675
nlTK--nlTK	NLTK versions before 3.10.3 contain a path sandbox bypass vulnerability in corpus-reader constructors that allows attackers to read files outside the intended data root. Attackers can supply arbitrary corpus root paths to LinThesaurusCorpusReader and PanLexLiteCorpusReader constructors to access filesystem content and SQLite databases outside the pathsec sandbox boundary.	2026-08-25	8.2	CVE-2026-79674
nlTK--nlTK	NLTK versions before 3.10.3 fail to use validated absolute paths when invoking the Graphviz dot binary in dependencygraph.dot2img and AlignedSent._repr_svg_.	2026-08-25	7.8	CVE-2026-78680

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allowing attackers to execute arbitrary code by placing a malicious dot binary in the search path or current working directory. Attackers can exploit bare-name binary resolution on Windows via the current working directory or on Unix-like systems via relative PATH entries to execute their binary instead of the legitimate Graphviz tool.			
nlTK--nlTK	NLTK versions before 3.10.3 use xml.etree.ElementTree to parse XML in multiple modules, which honors entity declarations in document DTDs. Attackers can craft XML payloads with nested entity declarations that expand from hundreds of bytes to megabytes in memory, causing denial of service.	2026-08-25	7.5	CVE-2026-78681
nlTK--nlTK	NLTK before 3.10.3 contains a server-side request forgery vulnerability in nltk.pathsec.urlopen (and callers nltk.data.load, nltk.downloader.Downloader.index/download) when an HTTP proxy is configured. pathsec.urlopen validates the requested hostname locally, but proxy-handler inheritance disables the safe HTTP/HTTPS handlers so the actual fetch is performed by the proxy against a destination that is never re-validated. An attacker can supply a validated public URL that the proxy forwards to an internal loopback-only service, allowing disclosure of internal HTTP resources, loading of forged downloader indexes, and installation of attacker-chosen package content.	2026-08-25	7.5	CVE-2026-78682
nlTK--nlTK	NLTK versions before 3.10.0 contain a regular expression denial of service vulnerability in Text.findall() and TokenSearcher.findall() methods that accept user-supplied regular expressions without validation or timeout. Attackers can supply crafted regex patterns that cause catastrophic backtracking, resulting in indefinite CPU saturation and denial of service to all users of the Python process.	2026-08-26	7.5	CVE-2026-80205
nlTK--nlTK	nltk PorterStemmer in versions <= 3.10.2 (fixed in 3.10.3) contains an inefficient-algorithmic-complexity denial of service in PorterStemmer.stem(). The _is_consonant() helper walks backward over the entire run of trailing 'y' characters on every call, and _measure() invokes it for each stem position, causing O(n^2) behavior. A single ~20-50 KB untrusted token consisting of a long run of the letter 'y' followed by a matching suffix (e.g., 'ness') can pin a CPU core for seconds to minutes, causing availability impact.	2026-08-27	7.5	CVE-2026-81722
nlTK--nlTK	NLTK through 3.10.3 contains a path traversal vulnerability in model-artifact APIs that bypass pathsec enforcement by using raw file operations on caller-controlled paths. Attackers can read or write files outside allowed sandbox roots through TransitionParser, AveragedPerceptron, PerceptronTagger, and maxent parameter APIs when pathsec is enabled.	2026-08-27	7	CVE-2026-81726
nlTK--nlTK	NLTK versions before 3.10.3 contain a filesystem containment bypass vulnerability in the Downloader.download and Downloader.incr_download methods that allows attackers to overwrite files outside the install root through pre-existing hardlinks. Attackers with write access to a shared downloader directory can create hardlinks pointing to outside-root files that are then overwritten during normal package extraction, mutating files outside the intended install tree.	2026-08-27	7.1	CVE-2026-81727
node-modules--urllib	urllib is an HTTP client for Node.js that supports authentication, redirects, timeouts, and other request features. Prior to 4.9.1 and 2.44.1, urllib follows redirects through followRedirect but reuses caller-supplied options across origins. In src/HttpClient.ts, #requestInternal recursively calls this.#requestInternal(nextUrl.href, options, requestContext), causing options.headers and auth or digestAuth values to be reused when the redirect target has a different scheme, host, or port. Authorization, Cookie, Proxy-Authorization, x-api-key, x-auth-token, and x-access-token can therefore be sent to an attacker-controlled redirected origin, exposing credentials intended for the original origin and potentially allowing reuse against the original partner API or related services. No user interaction is required. This issue is fixed in versions 2.44.1 and 4.9.1.	2026-08-25	7.5	CVE-2026-55553
Notification Master--Notification Master-Real-Time WordPress Notifications With Email, SMS, Webhooks & More	Unauthenticated Broken Access Control in Notification Master – Real-Time WordPress Notifications With Email, SMS, Webhooks & More <= 1.7.1 versions.	2026-08-24	7.5	CVE-2026-28153
NousResearch--hermes-agent	Hermes Agent 0.18.2 prior to 0.19.0 contains a supply chain vulnerability in its bundled MCP catalog that allows a remote attacker to execute arbitrary code by compromising a third-party upstream repository referenced via a mutable branch	2026-08-28	8.3	CVE-2026-82021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	rather than a pinned commit SHA. An attacker who compromises the upstream repository can propagate malicious code to every host that installs the affected catalog entry, with no further action required by the operator.			
NVIDIA--DGX Spark	NVIDIA DGX Spark contains a vulnerability in the system firmware, where a privileged attacker could be able to cause an out-of-bounds write. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	2026-08-25	8.2	CVE-2026-24262
NVIDIA--DGX Spark	NVIDIA DGX Spark contains a vulnerability in the system firmware, where a privileged attacker could be able to cause a NULL pointer dereference. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	2026-08-25	8.2	CVE-2026-24263
NVIDIA--DGX Spark	NVIDIA DGX Spark contains a vulnerability in the system firmware, where a privileged attacker could be able to cause an out-of-bounds write. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, denial of service, information disclosure, and data tampering.	2026-08-25	8.2	CVE-2026-47626
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its installation process, where an attacker could cause execution of untrusted code. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, information disclosure, and denial of service.	2026-08-25	8.1	CVE-2026-65081
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its deployment process, where an attacker could cause improper certificate validation. A successful exploit of this vulnerability might lead to information disclosure, data tampering, code execution, and escalation of privileges.	2026-08-25	8.1	CVE-2026-65084
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its remote-access helper workflow, where an attacker could cause weak authentication. A successful exploit of this vulnerability might lead to code execution, information disclosure, and data tampering.	2026-08-25	8.1	CVE-2026-65098
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its inference server setup, where a remote attacker may access the inference service without authentication. A successful exploit of this vulnerability may lead to information disclosure and denial of service.	2026-08-25	8.1	CVE-2026-65105
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its migration command, where a local attacker could cause code injection. A successful exploit of this vulnerability might lead to code execution, data tampering, information disclosure, and denial of service.	2026-08-25	7	CVE-2026-65082
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its status and logs plugin commands, where an attacker could cause OS command injection. A successful exploit of this vulnerability might lead to code execution, data tampering, information disclosure, and denial of service.	2026-08-25	7.8	CVE-2026-65089
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its NIM management component, where an attacker could cause OS command injection. A successful exploit of this vulnerability might lead to code execution, data tampering, information disclosure, and denial of service.	2026-08-25	7.8	CVE-2026-65090
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in the Telegram bridge component, where an attacker could cause an OS command injection. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	2026-08-25	7.8	CVE-2026-65096
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its installation scripts, where an attacker could cause a download of code without integrity check. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	2026-08-25	7.5	CVE-2026-65097
NVIDIA--NemoClaw	NVIDIA NemoClaw for Linux contains a vulnerability in its command-line interface, where an attacker could cause OS command injection. A successful exploit of this vulnerability might lead to code execution, data tampering, information disclosure, and denial of service.	2026-08-25	7.8	CVE-2026-65099
NVIDIA--OpenShell	NVIDIA OpenShell for Linux contains a vulnerability in its sandbox provisioning API, where an attacker could cause an incomplete list of disallowed inputs. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, data tampering, and denial of service.	2026-08-25	9.9	CVE-2026-65083
NVIDIA--OpenShell	NVIDIA OpenShell for Linux contains a vulnerability where an attacker could cause a sandbox escape. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-08-25	9.9	CVE-2026-65093
NVIDIA--OpenShell	NVIDIA OpenShell for all platforms contains a vulnerability where a malicious gateway could cause OS command injection. A successful exploit of this	2026-08-25	8.8	CVE-2026-65091

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability might lead to code execution, data tampering, and information disclosure.			
NVIDIA--OpenShell	NVIDIA OpenShell Sandbox for Linux contains a vulnerability where an attacker could cause a path traversal bypass of L7 REST network policy. A successful exploit of this vulnerability might lead to information disclosure and data tampering.	2026-08-25	8.5	CVE-2026-65092
NVIDIA--Unified Fabric Manager Enterprise - GA	NVIDIA UFM Enterprise contains a vulnerability in the plugin management API, where an authenticated user with low privileges could inject code by sending a specially crafted API request. A successful exploit of this vulnerability might lead to code execution, escalation of privileges and information disclosure.	2026-08-25	8	CVE-2026-24169
NVIDIA--Unified Fabric Manager Enterprise - GA	NVIDIA UFM Enterprise contains a vulnerability in the web interface authorization component, where an authenticated user could cause improper authentication by sending specially crafted HTTP requests. A successful exploit of this vulnerability might lead to code execution and escalation of privileges.	2026-08-25	8.8	CVE-2026-24170
oauth2-proxy--oauth2-proxy	OAuth2 Proxy honours a client-supplied X-Forwarded-Uri header when deciding whether a request may skip authentication, because the guard added for CVE-2026-40575 is inert in the default reverse-proxy configuration. GetRequestURI in pkg/requests/util/util.go prefers that header over the real request URI whenever CanTrustForwardedHeaders returns true, and isAllowedPath in oauthproxy.go matches the skip_auth_routes and skip_auth_regex allow list against the resulting path. CanTrustForwardedHeaders in pkg/apis/middleware/scope.go grants that trust when the caller's address is in the trusted proxy set, and buildTrustedProxyNetSet falls back to defaultTrustedProxyIPs, which is 0.0.0.0/0 and ::/0, whenever reverse proxy mode is enabled without trusted_proxy_ip configured. Every client is therefore treated as a trusted proxy. An unauthenticated attacker can request a protected upstream path while setting X-Forwarded-Uri to a value matching an allow-listed route, so the skip-auth decision is made against the spoofed value while the upstream receives the protected path unchanged.	2026-08-24	9.1	CVE-2026-76835
omnivore-app--omnivore	The Omnivore API (packages/api) before the fix in commit abf53d6 contains an authentication bypass in Apple sign-in token verification. The decodeAppleToken function extracted the 'alg' field from the attacker-supplied JWT header and passed it as the sole allowed algorithm to jwt.verify(). Using jsonwebtoken v8 (which does not validate key/algorithm compatibility), an attacker can set alg=HS256 and sign a forged token using Apple's publicly available RSA public key as the HMAC secret, bypassing signature verification and impersonating any Apple-linked account.	2026-08-29	9.1	CVE-2026-82454
onedesigns--One User Avatar User Profile Picture	The One User Avatar User Profile Picture plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.5.4 via the wpua_action_process_option_update function. This is due to insufficient file type validation in wp_handle_upload() called without a MIME allow-list, with post-write validation relying on the attacker-controlled client-supplied Content-Type header rather than a server-derived type, and no cleanup of files that fail the check. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload files that may be executable, which makes remote code execution possible. In order to exploit this vulnerability an admin has to give subscribers permission to upload avatars. While PHP files and svg files are rejected, dxfp files are accepted.	2026-08-28	7.5	CVE-2026-18983
OneUptime--OneUptime	OneUptime's webhook target check rejects private and loopback addresses given in IPv4 form and a small set of IPv6 forms, but has no case for the IPv4-mapped IPv6 range. The webhook delivery path calls SSRFPProtection.validateWebhookTargetIsSafe, and the host-literal screening inside Common/Server/Utils/SSRFPProtection.ts, performed by isBlockedHostnameLiteral, rejects private and loopback IPv4 ranges and tests an IPv6 value against the unspecified address, the loopback, the link-local prefix and the unique-local prefixes. A value such as [::ffff:127.0.0.1] matches none of them. The value is also recognised as an address literal rather than a name, so the path that re-checks addresses obtained from resolution is not taken. The HTTP client treats the mapped form as the embedded IPv4 address and connects to it, so an authenticated project member who can configure a webhook can direct the server at loopback services, private network ranges and link-local metadata endpoints, and the response is recorded where the webhook result can be read. Version 12.0.7 adds handling for the mapped range.	2026-08-26	7.1	CVE-2026-80350
open-metadata--OpenMetadata	OpenMetadata accepts a caller-supplied post-authentication redirect target and appends the issued token to it. SamlLoginServlet reads the callback request parameter and stores it in the HTTP session without comparing it against any configured or registered destination, and the assertion consumer servlet later	2026-08-26	8.1	CVE-2026-81029

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	formats that stored value into a URL carrying the freshly issued JWT together with the account's email and name before sending the redirect. The OIDC and OAuth2 handler follows the same pattern with its own redirect parameter and the issued identity token. A request naming a destination the attacker controls therefore causes the server to deliver a valid token for whoever completes the login to that destination. Because the token authenticates API calls as that account, a user who follows such a link and authenticates hands over control of their account. Version 2.0.0 removes the caller-supplied callback parameter; no 1.x release validates it.			
Open-Xchange GmbH--OX Dovecot Pro	An attacker that has valid credentials can use a Sieve script with the editheader extension to trigger a use-after-free in the mail editing code, and to write memory contents beyond the intended buffer into the delivered mail. This causes memory leak and opportunity to do memory corruption during mail delivery, which can crash the delivery process and may allow execution of arbitrary code in the context of that process. Disable the Sieve editheader extension. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	9.1	CVE-2026-42007
Open-Xchange GmbH--OX Dovecot Pro	An attacker that can send mail to a user can craft a message whose headers contain a very large number of email addresses or MIME parameters, which causes excessive memory usage when the message is later parsed. The message is still delivered, but reading it over IMAP can exhaust the memory limit of the process and terminate it, causing denial of service for the affected user. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	7.5	CVE-2026-27852
Open-Xchange GmbH--OX Dovecot Pro	An unauthenticated attacker can crash the ManageSieve login process by sending a small malformed command before authenticating. If running in high-security mode (default for community releases), only the attacker's own connection is terminated. If running in high-performance mode (default for Pro releases), all connections handled by the same managesieve-login process are terminated. Repeating the attack can cause denial of service for Sieve script management. Restrict network access to the ManageSieve service to trusted clients. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	7.5	CVE-2026-33605
Open-Xchange GmbH--OX Dovecot Pro	None None None No publicly available exploits are known.	2026-08-28	7.4	CVE-2026-40018
Open-Xchange GmbH--OX Dovecot Pro	An unauthenticated attacker can send an IMAP ID command with a very large number of parameters before logging in, which causes memory and CPU usage to grow disproportionately. The login process can be terminated by the out-of-memory handling, which also terminates all other connections handled by the same process. This can cause degradation or denial of service for IMAP logins. Limit the number of connections handled by a single imap-login process. This has a performance impact though. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	7.5	CVE-2026-42391
Open-Xchange GmbH--OX Dovecot Pro	An attacker that holds a token intended for a different purpose can authenticate, because when an OAuth2 token response does not contain a scope claim, the audience claim is used in its place and checked against the configured required scopes. These are different concepts, and the audience claim does not describe what a token is allowed to do. A token that grants no relevant permissions can be accepted because its intended recipient value happens to match a configured scope name, granting access that should have been denied. It also hides an identity provider misconfiguration where scopes are not being issued at all. Ensure the identity provider issues a scope claim for all tokens used with Dovecot, and that configured scope names do not match audience values. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	7.4	CVE-2026-73208
Open5GS--Open5GS	A vulnerability was detected in Open5GS 2.8.0. This affects the function pcrf_rx_aar_cb of the file src/pcrf/pcrf-rx-path.c of the component Rx AA-Request Handler. Performing a manipulation results in out-of-bounds read. It is possible to initiate the attack remotely. The patch is named c18dc6938bf63cc7374315d3dca303d92066e746. To fix this issue, it is recommended to deploy a patch.	2026-08-24	7.4	CVE-2026-78157
openNDS--openNDS	openNDS before 11.0.0 is susceptible to unauthenticated OS command execution via shell command injection through the fas query parameter on the /opennds_preauth/ endpoint because of libopennds.sh.	2026-08-28	8.3	CVE-2026-38820
openNDS--openNDS	A heap-based buffer overflow vulnerability exists in openNDS before 11.0.0 that allows an unauthenticated attacker on the captive portal network to crash the openNDS daemon (denial of service) and potentially achieve remote code execution. This is in http_microhttpd.c.	2026-08-28	7.1	CVE-2026-38821

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openNDS--openNDS	In openNDS before 11.0.0, the client_params.sh script, invoked by the openNDS daemon to serve the authenticated client status page, is vulnerable to OS command injection through crafted HTTP GET query parameter keys. An authenticated captive portal user can inject arbitrary shell commands by embedding semicolons in a URL query parameter name.	2026-08-28	7.6	CVE-2026-38822
openremote--openremote	OpenRemote versions before 1.28.0 contain a cross-realm information disclosure vulnerability in the Notification REST API that allows per-realm tenant administrators to read all tenants' sent notifications including message bodies. Attackers with read:admin credentials in one realm can submit a zero-parameter GET request to the notification endpoint to retrieve sensitive notification metadata and message content from all realms.	2026-08-27	7.7	CVE-2026-81679
optimole--Optimole Optimize Images Convert WebP & AVIF CDN & Lazy Load Image Optimization	The Optimole - Optimize Images Convert WebP & AVIF CDN & Lazy Load Image Optimization plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'a' (above_fold_images) parameter in all versions up to, and including, 4.2.10 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-28	7.2	CVE-2026-77365
oscal-compass--compliance-trestle	Compliance-trestle (Trestle) is a Python SDK and command-line tool for managing OSCAL compliance documents. In versions before 3.12.4 and versions 4.0.0 through 4.0.3, Trestle is vulnerable to server-side template injection that can lead to remote code execution. This occurs because the MDCleanInclude and MDSectionInclude Jinja2 tags re-parse untrusted Markdown content as template source code using a non-sandboxed jinja2.Environment. An attacker who controls content that Trestle renders, such as a crafted workspace Markdown file, a third-party SSP document, or a YAML lookup-table value, can inject a Jinja2 expression that traverses Python object internals to execute arbitrary operating system commands in the context of the Trestle process. This issue is fixed in versions 3.12.4 and 4.1.0.	2026-08-25	7.8	CVE-2026-54757
oscal-compass--compliance-trestle	Compliance-trestle (Trestle) is a Python SDK and command-line tool for managing OSCAL compliance documents. In versions prior to 3.12.4 and 4.0.0 through 4.0.3, the custom Jinja2 include tags mdsection_include and md_clean_include re-parse the content of an included Markdown file as Jinja2 template code in a non-sandboxed environment, allowing server-side template injection that can lead to arbitrary code execution. The MDSectionInclude and MDCleanInclude tags in Trestle/core/jinja/tags.py pass included file content to Parser(self.environment, ...).parse(), splicing it into the host template's compilation, and the environment is a plain jinja2.Environment rather than a SandboxedEnvironment, so any expressions in the file are evaluated with full access to the usual SSTI gadget chain. Because Trestle's Markdown writers emit OSCAL prose and component-description fields verbatim, applying delimiter neutralization only to parameter tables, attacker-controlled OSCAL data such as a control statement, part prose, or component description containing Jinja2 syntax flows into an included Markdown file and is executed when the include tag re-parses it. This issue is fixed in version 4.1.0.	2026-08-25	7.8	CVE-2026-57170
oscal-compass--compliance-trestle	Compliance-trestle (Trestle) is a Python SDK and command-line tool for managing OSCAL compliance documents. In versions before 3.12.4 and versions 4.0.0 through 4.0.3, the catalog-generate, profile-generate, and ssp-generate author commands write generated Markdown to an attacker-influenced output path without path-traversal validation, allowing arbitrary file write outside the Trestle workspace. These commands join the user-supplied output argument onto the Trestle root and write to the result, but guard it only with an is_directory_name_allowed() task-name-collision check rather than the PathSecurityValidator.validate_local_path() guard used by the jinja command, so an absolute path or one containing traversal sequences escapes the workspace and writes files under an attacker-chosen location as the invoking process owner. The security boundary is crossed when a trusted CI job, shared service, or wrapper derives the output argument from repository-controlled, tenant-controlled, or otherwise untrusted data while expecting output to stay inside the workspace. When --force-overwrite is used, the selected output directory is first recursively deleted, extending the primitive to destruction of an attacker-chosen directory tree and enabling indirect code execution by overwriting files a pipeline later runs. This issue is fixed in versions 3.12.4 and 4.1.0.	2026-08-25	7.7	CVE-2026-57171

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pac4j--pac4j	pac4j-oidc before 6.5.6 fails to verify access token signatures, issuers, audiences, or expiry when extracting Keycloak realm and client roles. Attackers can forge access tokens with administrative roles paired with valid ID tokens to bypass authorization checks in applications relying on pac4j role validation.	2026-08-29	8.1	CVE-2026-82461
pac4j--pac4j	pac4j-core before 6.5.6 contains an authentication bypass vulnerability in CheckProfileTypeAuthorizer that reverses the profile type validation logic. Attackers can authenticate through a weaker client and access resources requiring a stronger profile type by satisfying generic profile checks.	2026-08-29	8.1	CVE-2026-82463
Paolo--GeoDirectory	Unauthenticated Cross Site Request Forgery (CSRF) in GeoDirectory <= 2.8.176 versions.	2026-08-27	8.8	CVE-2026-81271
PayRange--PayRange API	PayRange API is missing proper authorization on management endpoints, which allows verbose details of every device on the PayRange network to be publicly accessible, with or without an account.	2026-08-27	8.8	CVE-2026-18965
penpot--penpot	Penpot is an open-source design and prototyping platform. In versions up to and including 2.14.3, Penpot is vulnerable to stored cross-site scripting through file comments, whose content is stored as raw text and rendered into the page with innerHTML without any sanitization. Because the backend applies only a length check and the frontend writes comment content directly through innerHTML, any team member who can comment on a shared file can embed HTML such as an image error handler or script that executes in the browser of every other collaborator. The attack is passive: any user who opens the comments panel on the affected file triggers script execution on the Penpot origin, allowing theft of session cookies, actions performed as the victim, and access to their files and projects. This issue is fixed in version 2.15.3.	2026-08-26	8.7	CVE-2026-47665
penpot--penpot	Penpot is an open-source design and prototyping platform. In versions up to and including 2.14.3, Penpot is vulnerable to stored cross-site scripting through custom font family names, which are interpolated into a @font-face CSS rule and injected into the page as HTML without sanitization. Because the backend accepts an arbitrary font-family string and the frontend writes the resulting style through innerHTML, a name containing markup such as a closing style tag followed by a script can break out of the style element and execute JavaScript on the Penpot origin. The attack is passive: any team member who opens a file referencing the malicious font triggers script execution simply by rendering the page, allowing theft of session cookies, actions performed as the victim, and access to their files and projects. This issue is fixed in version 2.15.3.	2026-08-26	7.6	CVE-2026-47666
phpipam--phpipam	phpIPAM before 1.8.2 contains an authentication bypass vulnerability in the REST API that allows unauthenticated attackers to gain full API access by exploiting an insecure object cache keying mechanism. The cache is keyed by lookup value alone without including the searched column, enabling an entry written during an app_id lookup to satisfy a subsequent app_code lookup, allowing attackers to use the numeric database row identifier as an API token to read, write, and delete all IP address management records.	2026-08-24	9.1	CVE-2026-67602
phpsysinfo--phpsysinfo	phpSysInfo is a customizable PHP script that displays system information. Prior to 3.4.6, the PSI_ALLOWED access-control check in read_config.php trusts attacker-controlled X-Forwarded-For and Client-IP HTTP headers before REMOTE_ADDR. A remote unauthenticated attacker can supply an allowed address in one of these headers to impersonate a trusted client and access exposed hostname, kernel, CPU, memory, filesystem, and network-interface information. This issue is fixed in version 3.4.6.	2026-08-28	7.5	CVE-2026-55584
piccolo-orm--piccolo_admin	Piccolo Admin is an admin interface and content management system for Python, built on top of Piccolo. Prior to 1.14.0, piccolo_admin/endpoints.py uses superuser_validators to block PUT, PATCH, DELETE, and POST requests by non-superusers but permits GET requests to configured user and session tables, while piccolo_api/session_auth/tables.py exposes SessionsBase.token because the token column is not secret. In deployments that add the Sessions and User tables to create_admin, a non-superuser administrator can call GET /api/tables/sessions/, obtain another user's live session token, replay it as the Cookie id value to impersonate a superuser, and permanently set superuser to true on the attacker's own row. This issue is fixed in version 1.14.0.	2026-08-28	8.8	CVE-2026-55485
pimcore--pimcore	Pimcore is an Open Source Data & Experience Management Platform. Prior to 11.5.19, 12.3.10, and 2026.1.6, the class-definition import endpoint /pimcore-studio/api/class/definition/configuration-view/detail/{id}/import accepts a DataObject field name that is emitted without an identifier allowlist by lib/DataObject/ClassBuilder/FieldDefinitionPropertiesBuilder.php into generated	2026-08-28	9.9	CVE-2026-55634

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	PHP properties and by models/DataObject/ClassDefinition/Helper/Dao.php into ALTER TABLE identifiers. An authenticated user with the objects permission can inject PHP syntax into the generated DataObject class, causing attacker-controlled code in generated var/classes/DataObject/.php files to run when an object of that class is instantiated, and can also inject SQL identifier content into schema-changing statements. The central models/DataObject/ClassDefinition/Data.php::setName() validation did not reject semicolons, braces, backticks, spaces, or other non-identifier characters. This issue is fixed in versions 11.5.19, 12.3.10, and 2026.1.6.			
PixelYourSite Professional--Boost	Unauthenticated SQL Injection in Boost <= 2.0.4 versions.	2026-08-24	9.3	CVE-2026-32555
PixelYourSite Professional--Boost	Unauthenticated Cross Site Scripting (XSS) in Boost <= 2.0.4 versions.	2026-08-24	7.1	CVE-2026-32556
PLANET Technology Corp.--PLANET GS-4210-16P2S	PLANET GS-4210-16P2S firmware before 3.441b260626 contains an authenticated OS command injection vulnerability in /cgi-bin/dispatcher.cgi. The web_vlan_membership_edit_dialog_post handler incorporates the memberTags POST parameter into a shell command without sanitization. A remote authenticated attacker can send a crafted memberTags value to execute arbitrary operating-system commands on the device.	2026-08-28	7.2	CVE-2026-75121
PLANET Technology Corp.--PLANET GS-4210-16P2S	PLANET GS-4210-16P2S firmware before 3.441b260626 contains an authenticated OS command injection vulnerability in /cgi-bin/httpuploadcert.cgi. The certificate password field in a certificate upload request is incorporated into a shell command without sanitization of shell metacharacters. A remote attacker with administrator web credentials can submit a crafted certificate upload request to execute arbitrary operating-system commands on the device.	2026-08-28	7.2	CVE-2026-75122
PLANET Technology Corp.--PLANET GS-4210-16P2S	PLANET GS-4210-16P2S firmware before 3.441b260626 contains an authenticated OS command injection vulnerability in /cgi-bin/dispatcher.cgi. The web_smtp_test_post handler incorporates a caller-supplied SMTP server value directly into a shell command without sanitization. A remote attacker with administrator web credentials can send a crafted SMTP server value to execute arbitrary operating-system commands on the device.	2026-08-28	7.2	CVE-2026-75123
PLANET Technology Corp.--PLANET GS-4210-16P2S	PLANET GS-4210-16P2S firmware before 3.441b260626 contains a pre-authentication memory corruption vulnerability in the web management interface where the _readHttpParam function copies an oversized HTTP query string without guaranteeing NUL termination, allowing parse_query_string to process attacker-controlled data into a fixed-size stack buffer. An unauthenticated remote attacker can send an oversized GET request to dispatcher.cgi to cause denial of service of the web management interface and potentially trigger memory corruption.	2026-08-28	7.5	CVE-2026-75124
plone--plone.app.event	plone.app.event provides the event content type for Plone. Prior to versions 5.2.4 and 6.0.1, the iCalendar import in src/plone/app/event/ical/importer.py accepts insufficiently restricted calendar and event URLs, does not adequately bound downloaded bytes or imported events, and commits work per event. A logged-in editor can make the server request internal network resources or local calendar files, exhaust resources and take the site offline, and store a malicious event URL that executes script in another user's browser. The fix restricts accepted URLs, applies MAXIMUM_ICAL_IMPORT_SIZE_BYTES and MAXIMUM_ICAL_IMPORT_EVENTS limits, uses transaction savepoints, and validates event URLs. This issue is fixed in versions 5.2.4 and 6.0.1.	2026-08-28	9.1	CVE-2026-55247
plone--plone.app.portlets	plone.app.portlets provides portlets and a Plone-specific user interface for plone.portlets. Prior to 5.0.8, 6.0.4, and 7.0.2, a member who can add an RSS portlet can set its feed URL to a very large response, causing src/plone/app/portlets/portlets/rss.py to download and retain excessive data in memory and deny service. The same RSS URL handling accepts internal hosts, IP addresses, single-word domains, and explicit ports, allowing server-side requests that can probe internal network services and open ports. A malicious feed item can also supply a JavaScript URL that is retained as the item link and can execute script when used by a victim. The affected logic includes _rss_feed_url_validator, _normal_url_validator, RSSFeed._retrieveFeed, RSSFeed._buildItemDict, and the FEED_DATA in-memory cache. This issue is fixed in versions 5.0.8, 6.0.4, and 7.0.2.	2026-08-28	9.1	CVE-2026-55248
Portkey-AI--gateway	Portkey AI Gateway through 1.15.2 contains a server-side request forgery vulnerability in the /v1/proxy/* route that lacks requestValidator middleware. Attackers can set the x-portkey-custom-host header to internal addresses and	2026-08-28	7.5	CVE-2026-82270

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	forward requests with Authorization headers to reach internal services and exfiltrate provider API keys.			
pteroactyl--wings	Wings is the server control plane for the Pterodactyl game-server management panel. In versions up to and including 1.13.2, the SFTP write path does not enforce a server's disk quota during a transfer, allowing a tenant with SFTP write access to a single server to exhaust the host node's physical disk and take down every server on it. Wings checks available space only once, as a boolean, when the write handle is opened, using a stale cached usage value and without knowing the size of the incoming data, and it then returns a raw, unaccounted file handle that is never re-checked as the transfer proceeds. A single upload can therefore be written without bound, far beyond the configured disk limit, until the node's disk is full, and because a server stopped for exceeding its limit is not treated as suspended, SFTP writes are still accepted even after the quota is already exceeded. This issue is fixed in version 1.13.3.	2026-08-26	7.7	CVE-2026-61617
Qubes OS--Qubes OS	Qubes OS before qubes-core-dom0-linux 4.3.22 allows OS command injection during a qvm-copy-to-vm call from dom0 to an attacker-controlled qube, because the "system" library function is used to process an error message that may have shell metacharacters. This occurs in core-admin-linux/file-copy-vm/qfile-dom0-agent.c.	2026-08-30	7.9	CVE-2026-82636
QuivrHQ--quivr	Quivr versions through 0.0.322 fail to validate chat ownership in the GET /chat/{chat_id}/history, DELETE /chat/{chat_id}, and POST /chat/{chat_id}/question/answer endpoints. Authenticated attackers can read other users' conversation histories including private knowledge base content, delete arbitrary chats, and inject fabricated messages into other users' conversations.	2026-08-28	8.1	CVE-2026-82284
QuivrHQ--quivr	Quivr through 0.0.322 fails to validate ownership in prompt endpoints, allowing authenticated users to modify any prompt by identifier. Attackers with read-only access to shared brains can read exposed prompt identifiers and overwrite system prompts affecting all brain users.	2026-08-28	7.1	CVE-2026-82280
QWED-AI--qwed-mcp	QWED-MCP is a deterministic verification gateway for MCP. Prior to 0.2.1, verify_math_expression() in src/qwed_mcp/engines/math_engine.py passes attacker-controlled expression and claimed_result strings directly to SymPy's parse_expr() after only normalizing caret syntax to Python exponent syntax, without restricting global_dict, removing Python built-ins, or validating the expression AST. Because parse_expr() calls Python's eval() with built-ins available, an attacker who can cause a downstream caller to pass untrusted input to this public library function can use Python import functionality to execute arbitrary operating-system commands as the qwed-mcp process user, read or modify accessible data, exfiltrate process secrets, or reach internal services. The default MCP tool registry does not expose verify_math_expression(), so exploitation requires a downstream integration that invokes the library API with attacker-controlled input. This issue is fixed in version 0.2.1.	2026-08-25	9.8	CVE-2026-55546
QWED-AI--qwed-verification	QWED is open-source AI verification infrastructure for deterministic verification of LLM outputs, tool calls, code, schemas, and agent state before production execution. Prior to 5.1.2, the qwed package passes caller-controlled math expressions directly to SymPy parse_expr() without restricted global_dict and local_dict namespaces, allowing Python eval() to resolve builtins and execute arbitrary Python code in the API server process. In src/qwed_new/api/main.py, POST /verify/math is protected by get_current_tenant but accepts any valid tenant API key, reads the expression field, applies only a cosmetic re.sub(r'(\d){1}', r'\1*\2', expression) normalization, and passes the result to parse_expr(). In src/qwed_new/core/batch.py, POST /verify/batch sends math items through batch_service.create_job(), stores item.query verbatim, and _verify_item() passes VerificationType.MATH input to parse_expr() without sanitization. The default-enabled POST /auth/signup endpoint allows anyone to create a standard tenant account, POST /auth/api-keys issues an x-api-key, and either vulnerable path can then be used to read or write files, modify data, execute operating system commands, terminate the service, and compromise other tenants in a shared deployment. This issue is fixed in version 5.1.2.	2026-08-25	8.8	CVE-2026-55585
QwenLM--Qwen-Agent	Qwen-Agent through 0.0.34 contains a server-side request forgery vulnerability in the document parsing path that treats caller-supplied paths as URLs without scheme restriction or host validation. Attackers can reach the unauthenticated Gradio interface to make the server issue HTTP requests to arbitrary internal	2026-08-28	7.5	CVE-2026-82268

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	addresses including metadata services and read retrieved content through parsed document output.			
QwenLM--Qwen-Agent	Qwen-Agent through 0.0.34 contains a path traversal vulnerability in the document parser that fails to restrict file access to intended directories. Attackers can supply absolute file paths to the unauthenticated Gradio interface to read arbitrary files accessible by the server process.	2026-08-28	7.5	CVE-2026-82275
ractivejs--ractive	A weakness has been identified in ractivejs ractive up to 1.4.4. Impacted is the function Ractive#set of the component Keypath Handler. Executing a manipulation can lead to improperly controlled modification of object prototype attributes. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-24	7.3	CVE-2026-78181
RadiusTheme, LLC--ShopBuilder Pro Elementor WooCommerce Builder Addons	Unauthenticated Arbitrary File Deletion in ShopBuilder Pro - Elementor WooCommerce Builder Addons <= 2.2.0 versions.	2026-08-24	8.6	CVE-2026-32477
RadiusTheme--Classified Listing - Mobile Number Verification	The Classified Listing - Mobile Number Verification plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.6.0. This is due to missing server-side Firebase OTP validation in the process_otp_login() function. This makes it possible for unauthenticated attackers to authenticate as any user with a phone number registered in the plugin's phone table by submitting an arbitrary OTP code and UID through the Firebase OTP login flow. Successful exploitation requires OTP login to be enabled with Firebase selected as the verification gateway, and requires the attacker to know or guess the target account's registered phone number. Administrator account takeover is possible if an administrator account has a phone number registered in the plugin.	2026-08-26	8.1	CVE-2026-15985
Rank Math SEO--Rank Math SEO	Author Remote Code Execution (RCE) in Rank Math SEO <= 1.0.276 versions.	2026-08-28	7.2	CVE-2026-81757
Rapid7--Velociraptor	The Velociraptor verify() VQL function allows a user to verify an artifact for syntactic and other issues. Due to an implementation fault in this VQL function, the global artifact repository is used which allows callers to overwrite existing artifacts without the required permissions. The attacker need only have the NOTEBOOK_EDIT permission (e.g. an analyst role) to be able to call this function.	2026-08-24	8.9	CVE-2026-19200
rconfig--rconfig	rConfig Core 8.0.0 before 8.2.10 contains an authentication bypass vulnerability that allows unauthenticated attackers to self-register accounts with full Administrator privileges due to a duplicate bare Auth::routes() call in routes/web.php that re-enables the POST /register route after it was explicitly disabled. Attackers can register a new account that is immediately authenticated with Admin-level access because the registration controller does not assign a role and the users.role column defaults to Admin, enabling access to stored device credentials, user data, and API token issuance.	2026-08-24	9.8	CVE-2026-77915
Readabler--Readabler	The Readabler plugin for WordPress is vulnerable to SQL Injection in all versions up to 2.0.18 (exclusive) due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-25	7.5	CVE-2026-78576
readest--readest	Readest is an open-source e-book reader built on Tauri. In versions prior to 0.11.16, EPUB chapter HTML is sanitized with DOMPurify using a configuration that forbade only the <script> tag (FORBID_TAGS: ['script']) in apps/readest-app/src/services/transformers/sanitizer.ts. DOMPurify does not parse the contents of the srcdoc attribute on <iframe> elements, treating it as an opaque string attribute, so an attacker who can get an <iframe> element to survive sanitization can embed a complete HTML document containing a <script> tag inside srcdoc and have it execute when the browser renders the iframe. The content iframe is configured with sandbox="allow-same-origin allow-scripts", so script executing inside it shares the parent origin and can reach parent.parent.__TAURI_INTERNALS__.invoke(...), giving access to every Tauri IPC command the application is permitted to use, which escalates to arbitrary code execution. The payload can be made invisible (zero-size, transparent iframe) so the reader sees only normal book text. Version 0.11.16 hardened the sanitizer configuration by adding 'iframe', 'object' and 'embed' to FORBID_TAGS and adding 'srcdoc' to FORBID_ATTR.	2026-08-30	8.8	CVE-2026-82642

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Realtyna--Realtyna Organic IDX plugin	Unauthenticated Cross Site Scripting (XSS) in Realtyna Organic IDX plugin <= 5.4.1 versions.	2026-08-27	7.1	CVE-2026-78261
Red Hat--Red Hat Ansible Automation Platform 2.5 for RHEL 8	A path traversal vulnerability was found in AWX's project archive extraction. The project_archive action plugin extracts zip and tar archive members by joining the project directory path with the member filename without performing path normalization, boundary validation, or rejecting directory traversal sequences. A malicious archive containing members with path traversal components can write files to arbitrary locations on the execution node's filesystem outside the intended project directory. An attacker who controls the archive content, either through a compromised upstream source, a malicious archive URL, or a man-in-the-middle attack on a plain HTTP connection, can achieve arbitrary file writes as the user performing the extraction, potentially leading to remote code execution through mechanisms such as cron files, SSH authorized keys, or playbook content injection.	2026-08-24	7.2	CVE-2026-71364
Red Hat--Red Hat Ansible Automation Platform 2.5 for RHEL 8	A server-side request forgery (SSRF) vulnerability was found in multiple AWX notification backends. The webhook, Mattermost, Rocket.Chat, and Grafana notification backends use notification template URLs as direct HTTP request targets without validating the target address against private, loopback, or reserved IP ranges. An organization notification administrator can create notification templates pointing to internal or loopback addresses, causing the AWX control node to issue HTTP requests to services that are not externally accessible. Additionally, the webhook notification backend follows HTTP redirects and resends configured Basic Authentication credentials to redirect targets regardless of host change, allowing an attacker to exfiltrate notification credentials by redirecting to an attacker-controlled host. The Grafana backend sends its API key in the Authorization header to the configured target URL.	2026-08-24	7.7	CVE-2026-71366
Red Hat--Red Hat build of Apache Camel for Spring Boot 4	A flaw was found in Undertow. A remote attacker could exploit this vulnerability by sending specially crafted WebSocket messages with permessage-deflate negotiated. This could lead to excessive memory consumption due to the PerMessageDeflateFunction.largerBuffer() method using exponential doubling, resulting in a Denial of Service (DoS) for the affected application.	2026-08-27	7.5	CVE-2026-5680
Red Hat--Red Hat Enterprise Linux 10	NetworkManager did not apply the private_user restriction to the 802-1x.ca-path and phase2-ca-path directory-valued connection properties. This incomplete fix for CVE-2025-9615 allows an unprivileged local user to point a private WPA-Enterprise (802.1X) connection profile's CA path at an attacker-controlled directory, bypassing server certificate validation and enabling credential theft via a rogue access point.	2026-08-24	7.1	CVE-2026-19685
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in rsyslog. An unauthenticated remote attacker can trigger a heap buffer overflow in the RainerScript `replace()` function by sending specially crafted syslog messages. This vulnerability arises from an incorrect buffer size calculation during string replacement, causing memory corruption. Successful exploitation can lead to a denial of service (DoS) for the affected system.	2026-08-27	7.5	CVE-2026-78002
Red Hat--Red Hat Enterprise Linux 10	A vulnerability was found in RPM's rpmbuild tarball processing. When processing a crafted source archive, the getTarSpec() function in tools/rpmbuild.cc passes an attacker-controlled tar archive member name to rpmExpand() as part of a %{basename:...} macro expression. A specially crafted .spec member name can therefore inject RPM macros, including Lua expressions, resulting in arbitrary code execution with the privileges of the user running rpmbuild. This can be exploited when a victim or automated build system processes an attacker-controlled source tarball using rpmbuild tarball mode (such as -ts, -ta, or -tb).	2026-08-24	7	CVE-2026-78367
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in sos clean, a utility within the sos package. This vulnerability allows a local attacker to perform arbitrary file creation or overwrite. By crafting a malicious tar archive, an attacker can exploit a path traversal issue during tar extraction, where symlink and hardlink targets are not properly validated. This enables the attacker to write files to arbitrary locations on the system with the privileges of the sos clean process, which often runs as root.	2026-08-25	7.8	CVE-2026-79655
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in Emacs TRAMP. A local attacker could exploit this vulnerability by processing maliciously crafted filenames. This occurs because TRAMP concatenates login arguments without proper sanitization, which are then passed to a local shell. Successful exploitation could lead to arbitrary code execution.	2026-08-25	7.8	CVE-2026-79992
Red Hat--Red Hat Enterprise Linux 10	A stack-based buffer overflow vulnerability exists in BlueZ, the Linux Bluetooth protocol stack. A remote user within Bluetooth radio range can send a specially crafted Extended Inquiry Response (EIR) packet that causes a buffer overflow when the target device performs Bluetooth discovery. This vulnerability can lead to a Denial of Service (DoS) by crashing the bluetoothd service and may allow for arbitrary code execution.	2026-08-25	7.6	CVE-2026-80186

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
RedefiningTheWeb --Affiliate Pro - Affiliate Program for WooCommerce & WordPress	Unauthenticated Privilege Escalation in Affiliate Pro - Affiliate Program for WooCommerce & WordPress <= 8.9.1 versions.	2026-08-24	9.8	CVE-2026-32558
Redis--Redis	Redis contains a use-after-free vulnerability in the 'tlsProcessPendingData()' function, which handles the TLS pending-data list if Redis is configured with TLS support. A remote, unauthenticated attacker may be able to execute arbitrary commands with the privileges of the Redis server. Fixed in Redis 8.2.9, 8.4.6, 8.6.6, 8.8.2, and 8.10.1.	2026-08-27	9.8	CVE-2026-81934
redpanda-data--redpanda	Redpanda through 26.2.2 binds the Admin API to 0.0.0.0:9644 with admin_api_require_auth defaulting to false, treating unauthenticated requests as superusers. Attackers can reach port 9644 without credentials to create and delete broker accounts, modify cluster configuration, and disrupt partition replication.	2026-08-28	9.8	CVE-2026-82266
Rently--Smart Home	Rently Smart Home versions 20.1.0 and prior are vulnerable to an Insufficiently Protected Credentials vulnerability. This could allow an attacker to retrieve pins including the Master Pin, overriding standard user permissions.	2026-08-26	8.1	CVE-2026-75960
roxnor--ShopEngine Elementor WooCommerce Builder Addon All in One WooCommerce Solution with eCommerce Templates & Woo Widgets	The ShopEngine Elementor WooCommerce Builder Addon - All in One WooCommerce Solution plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 4.9.4. This is due to the 'rum_importer()' function being registered on the WordPress core 'import_start' action hook with no plugin-owned capability check and no allowlist filtering, causing arbitrary '<wp_option>' name/value pairs parsed from an attacker-supplied WXR import file to be passed directly to 'update_option()'. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to write arbitrary WordPress options - most critically setting 'users_can_register' to '1' and 'default_role' to 'administrator' - enabling open self-registration of Administrator accounts and full site takeover. This is exploitable by Shop Manager-level users because WooCommerce grants that role the 'import' capability, allowing it to reach the WordPress Importer flow that fires the 'import_start' hook on which 'rum_importer()' is registered, contrary to the assumption that the hook is restricted to Administrators.	2026-08-25	7.2	CVE-2026-75971
Ruby--resolv	An issue was discovered in the resolv gem before 0.7.2 for Ruby. Resolv::DNS::Resource.get_class, Resolv::DNS::Resource::Generic.create, and Resolv::DNS::SvcParam::Generic.create generate a new class for each unknown DNS resource record (type, class) pair, or each unknown SvcParamKey, encountered while decoding a response. Each generated class was permanently registered both as a constant on Resource (or SvcParam::Generic) and as an entry in a class-lookup hash (ClassHash), and thus the class remained reachable through that constant after the response was discarded. Type and class are each 16-bit values, and thus an attacker controlling DNS responses (a spoofed response, or a malicious or hijacked upstream DNS server) has roughly 2^32 distinct (type, class) pairs to choose from. A single response of a few hundred kilobytes carrying tens of thousands of distinct unknown types permanently grows process memory by tens of megabytes; repeated responses accumulate without bound and are never reclaimed by garbage collection, because the constant keeps each class alive. Any code path that calls Resolv::DNS::Message.decode on attacker-influenced DNS responses is affected. resolv is a default gem, and thus this is reachable from a plain Ruby installation without any additional dependency.	2026-08-27	7.5	CVE-2026-80212
ruby--rubygems	RubyGems fails to re-validate path containment after filesystem symlink resolution during gem extraction. When a pre-existing symlink inside the destination directory points outside the extraction root, extracted files that appear to be written under the destination directory can instead be written outside of it, breaking the extraction safety boundary. The fix resolves the real path of the parent directory before writing and raises Gem::Package::PathError if it escapes the destination directory.	2026-08-29	7.1	CVE-2026-82455
runatlantis--atlantis	Atlantis through 0.47.1 fails to authenticate the /github-app/setup endpoint, allowing unauthenticated attackers to access GitHub App credentials. Attackers can observe or intercept the GitHub redirect during setup to obtain the RSA private key and webhook secret, enabling installation token minting and webhook payload forgery.	2026-08-28	8	CVE-2026-82282
rustdesk--rustdesk	RustDesk's Windows clipboard redirection copies a peer-supplied length into a fixed-size caller buffer without an upper bound check. When an OLE paste consumer such as explorer.exe calls IStream::Read with a buffer of cb bytes,	2026-08-24	9.6	CVE-2026-76840

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ClipdrStream_Read in libs/clipboard/src/windows/wf_clipdr.c requests that many bytes of a remote file through clipdr_send_request_filecontents and then executes CopyMemory(pv, clipboard->req_fdata, clipboard->req_fsize), where req_fsize is taken verbatim from the peer's CLIPDR FileContentsResponse by wf_clipdr_server_file_contents_response (req_fsize = fileContentsResponse->cbRequested) and is never clamped to cb anywhere in the chain. The function's only length comparison, req_fsize < cb, handles the short-read case and is evaluated after the copy has already occurred. A malicious or compromised peer that answers a small file-contents read with an oversized response therefore writes attacker-chosen data past the end of the paste consumer's heap buffer when the local user pastes clipboard file contents offered by the remote side. The file is a fork of FreeRDP's client/Windows/wf_clipdr.c, where the same defect is CVE-2026-68579, fixed in FreeRDP 3.30.0.			
rustdesk--rustdesk	RustDesk versions before 1.4.7 contain an uncontrolled speculative memory allocation vulnerability in BytesCodec. Before authentication, the decoder trusts the payload length encoded in a four-byte frame header and reserves that amount before receiving the payload. A crafted header can request up to 1,073,741,823 bytes of capacity, allowing unauthenticated attackers to use concurrent TCP connections to cause memory exhaustion and denial of service. The fix caps header-triggered speculative preallocation at 256 KiB.	2026-08-26	7.5	CVE-2026-73108
ruvnet--sublinear-time-solver	sublinear-time-solver is a Rust and WebAssembly library for solving asymmetric diagonally dominant systems in sublinear time. Prior to consciousness-explorer 1.1.2 and sublinear-time-solver 1.6.0, the export_state and import_state tools in src/consciousness-explorer/mcp/server.js pass the attacker-controlled filepath parameter to filesystem operations in src/consciousness-explorer/index.js without restricting the destination or rejecting traversal. The saveVectorToFile and loadVectorFromFile tools in src/mcp/server.ts contain the same sink class through the file_path parameter. An attacker able to invoke the MCP tools can read, write, or overwrite any file accessible to the server process, causing confidentiality and integrity loss and possible service disruption. This issue is fixed in consciousness-explorer 1.1.2 and sublinear-time-solver 1.6.0.	2026-08-25	7.1	CVE-2026-55609
rybbit-io--rybbit	Rybbit before 2.7.0 contains a CORS misconfiguration vulnerability that allows attackers to bypass origin restrictions by reflecting any request origin in Access-Control-Allow-Origin responses while credentials are enabled. Attackers can issue credentialed cross-origin requests from any website to read analytics data, account information, and perform authenticated state-changing operations as the victim user.	2026-08-28	8.1	CVE-2026-82287
SAP_SE--SAP S/4HANA (Manage Supply Protection)	SAP S/4HANA (Private Cloud) uses a third-party component that contains a Regular Expression Denial of Service (ReDoS) vulnerability. An unauthenticated attacker could supply specially crafted input that triggers excessive processing within the affected functionality. Successful exploitation could exhaust system resources and make the service unavailable, resulting in a high impact on availability. There is no impact on confidentiality and integrity.	2026-08-25	7.5	CVE-2026-66766
seaweedfs--seaweedfs	SeaweedFS is a distributed storage system for files and blobs. In versions from 3.88 through 4.39, the SFTP server evaluates configured path permissions with a literal string-prefix comparison, so a user scoped to a path is also granted the same access to any sibling path whose name merely begins with the same characters. A user granted access to /tenants/alice therefore also matches /tenants/alice-archive, /tenants/alice2, and similar siblings, because the check does not require a path-component boundary. An authenticated low-privilege SFTP user with a root home directory and narrow path permissions can thereby cross the configured ACL boundary to read another tenant's files, and to overwrite them if granted write, all through the documented SFTP service with its own valid credentials. This issue is fixed in version 4.40.	2026-08-26	8.1	CVE-2026-77317
seaweedfs--seaweedfs	SeaweedFS is a distributed storage system for files and blobs. In version 4.39, the filer's TUS resumable-upload handler checks JWT allowed_prefixes scoping only when a session is created, letting a low-privilege tenant hijack another tenant's upload session to write content to filer paths their own token forbids. The HEAD, PATCH, and DELETE verbs that act on an existing session by its id never verify that the session's stored target path falls within the caller's allowed prefixes, so a tenant who obtains another upload's session identifier can PATCH attacker bytes into it and, on completion, have the file land at the victim's out-of-scope path. The same token can also DELETE other tenants' sessions and HEAD them to read upload progress and size, defeating the JWT prefix isolation. This vulnerability only affects	2026-08-26	7.6	CVE-2026-77368

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	deployments that configure filer JWT signing and have TUS uploads enabled. This issue is fixed in version 4.40.			
seaweedfs--seaweedfs	SeaweedFS is a distributed storage system for files and blobs. In versions prior to 4.40, an authenticated S3 principal with permissions scoped to a nested object key can overwrite a different object outside that scope by calling PutObjectAcl on the key it is allowed to access. The handler authorizes the request against the requested nested key but then writes the updated entry back to the bucket root rather than the key's actual parent directory, so an ACL change on allowed/protected.txt is instead applied to protected.txt at the bucket root. Because the update carries the full entry rather than only ACL metadata, an existing target object is overwritten with the content, metadata, owner information, and ACL of the scoped object, bypassing the object-level action scoping configured through the static S3 identity file. This issue is fixed in version 4.40.	2026-08-26	7.1	CVE-2026-77611
Select-Themes--Tonda	Unauthenticated Local File Inclusion in Tonda < 2.6 versions.	2026-08-24	8.1	CVE-2026-28151
Select-Themes--Tonda Core	Unauthenticated Local File Inclusion in Tonda Core < 2.6 versions.	2026-08-24	8.1	CVE-2026-28152
senaite--senaite.core	SENAITE.CORE is the core framework for the SENAITE laboratory information management system. From 2.0.0 to 2.6.0, the SENAITE.CORE JSON API permits unauthenticated remote code execution through a two-request chain involving missing authorization and unsafe evaluation. The state-changing routes in src/bika/lims/jsonapi/update.py, including update, update_many, remove, doActionFor, doActionFor_many, and getusers, do not enforce the senaite.core: Access JSON API permission before resolving attacker-selected objects. In src/bika/lims/jsonapi/init.py, set_fields_from_request passes raw request values for RecordsField and RecordField instances to eval() before field mutator write-permission checks execute. An anonymous attacker can discover the bika_setup object identifier through @@uuid, send a value such as RejectionReasons to /@@API/update, and execute arbitrary Python in the Zope worker before a later mutation failure rolls back ZODB changes. The same unsafe evaluation pattern is present in src/senaite/core/browser/fields/record.py and src/senaite/core/browser/fields/records.py. Successful exploitation can expose or modify laboratory data, files, and accounts and can disrupt the service.	2026-08-26	9.8	CVE-2026-54569
servmask--All-in-One WP Migration and Backup	The All-in-One WP Migration and Backup plugin for WordPress is vulnerable to SQL Injection via archive restore functionality in all versions up to, and including, 7.109 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This can be leveraged to obtain the ai1wm_secret_key when a site administrator performs an archive restore and achieve remote code execution once able to leverage the ai1wm_secret_key value.	2026-08-25	8.8	CVE-2026-19949
Shenzhen Gongji Technology--XBROTHER Dynamic Environment Monitoring System	A security vulnerability has been detected in Shenzhen Gongji Technology XBROTHER Dynamic Environment Monitoring System up to 300R004C00B300. The affected element is the function PlanController.getImmediatePlans of the file /xbreport/api/v1/plamange/plansImmediate. The manipulation of the argument order/sort leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	2026-08-24	7.3	CVE-2026-78182
Shinobi Systems--Shinobi	Shinobi before commit 5a76c74f contains a hardcoded connection key in the child node service that allows unauthenticated attackers to execute arbitrary database queries. Attackers reaching the child node port can present the hardcoded key during WebSocket handshake, then dispatch SQL queries through the onWebSocketDataFromChildNode handler to read and modify user records and camera configuration.	2026-08-29	9.8	CVE-2026-82448
Siemens--Element maps-ng V47	A vulnerability has been identified in Element maps-ng V47 (All versions < V47.12.3), Element maps-ng V48 (All versions < V48.11.3), Element maps-ng V49 (All versions < V49.16.1). The si-map component does not properly neutralize user-controllable input of the points property that is used to render the tooltip label of map pins. This could allow an attacker to craft a malicious URL that, when loaded by a victim and the map pin is hovered over, executes arbitrary script code within the victim's browser session.	2026-08-27	7.6	CVE-2026-66155

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SililaWijesinghe--Food Ordering System	A vulnerability was found in SililaWijesinghe Food Ordering System up to ba314e897e3365600461e5ea59432e39ceaa0fa5. Affected by this issue is some unknown functionality of the file /search.php. Performing a manipulation of the argument search_box results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-25	7.3	CVE-2026-79804
silverstripe--silverstripe-advancedworkflow	Silverstripe Advanced Workflow is a highly configurable step-based workflow module. Prior to 6.4.5, 7.1.3, and 7.2.1, an attacker with permission to author the advanced workflow email template can place a specially crafted server-side template payload in NotifyUsersWorkflowAction.EmailTemplate. When NotifyUsersWorkflowAction renders the field through the Silverstripe template engine SSTemplateParser, the payload can cause PHP evaluation and arbitrary code execution on the server; the regression coverage is in tests/php/WorkflowEngineTest.php. This issue is fixed in versions 6.4.5, 7.1.3, and 7.2.1.	2026-08-27	7.2	CVE-2026-54718
silverstripe--silverstripe-userforms	Silverstripe UserForms provides a visual form builder for the Silverstripe CMS. From 6.0.0 until 6.4.9, 7.0.7, and 7.1.1, the userform email recipient subject field in the CMS accepts a specially crafted payload that can be interpreted as executable server-side code. An authenticated CMS user with permission to configure a UserForms email recipient can use the subject field to run arbitrary code on the server, compromising confidentiality, integrity, and availability. This issue is fixed in versions 6.4.9, 7.0.7, and 7.1.1.	2026-08-27	8.8	CVE-2026-54721
SimpleMachines--SMF	Simple Machines Forum (SMF) through 2.1.7, fixed in commit 6f0dc61, contains an authorization state-confusion vulnerability in the profile loader that allows authenticated low-privileged users to gain administrator access by supplying multiple values for the user parameter. Attackers can exploit the mismatch between Profile::\$member and User::\$me->is_owner during sequential profile loading to be treated as the owner of an administrator profile, enabling unauthorized password changes and full account takeover.	2026-08-26	8.1	CVE-2026-43621
Site Building with Toolset--Toolset Blocks	Unauthenticated Cross Site Scripting (XSS) in Toolset Blocks <= 1.6.26 versions.	2026-08-24	7.1	CVE-2026-78264
siyuan-note--siyuan	SiYuan versions before v3.8.1 contain a server-side request forgery vulnerability in the http_request and web_fetch agent tools that perform DNS resolution only at guard time without validating the connect-time resolution. Attackers can use DNS rebinding to answer the guard resolution with a public IP and the connect resolution with a private or metadata IP, bypassing the SSRF defense to access cloud instance metadata and internal services.	2026-08-28	8.2	CVE-2026-82234
siyuan-note--siyuan	SiYuan before v3.8.1 contains a stored cross-site scripting vulnerability in confirmDialog() where unescaped package names and notebook names are interpolated directly into innerHTML assignments. Attackers can submit malicious bazaar packages with HTML/script payloads in the name field that execute in users' browsers when uninstalling packages or unlocking encrypted notebooks.	2026-08-30	8.9	CVE-2026-82653
siyuan-note--siyuan	SiYuan before v3.8.1 fails to properly escape block name, alias, and memo fields in hint, backlink, and breadcrumb rendering functions. Attackers can set a block's name to contain HTML/script tags that execute when another user views documents referencing or displaying that block.	2026-08-30	8.9	CVE-2026-82654
Skyvern-AI--skyvern	Skyvern before 1.0.45 contains a sandbox escape vulnerability in TextPromptBlock that renders prompts twice, first through a sandboxed Jinja environment and then through an unsandboxed environment. Attackers can inject malicious Jinja template syntax through workflow parameters or upstream block output to execute arbitrary code with server process privileges.	2026-08-29	8.8	CVE-2026-82447
snyk--sweater-comb	Synk Sweater Comb before 3.8.8 contains a command injection vulnerability that allows an attacker who controls the .vervet.yaml configuration file to execute arbitrary OS commands by injecting malicious input into the linters.<key>.optic-ci.original branch name field. The expectGitBranch() function in src/lint.ts passes the unsanitized branch name directly into child_process.exec() via an unescaped template literal, enabling arbitrary command execution when the lint command is run against the repository.	2026-08-28	8	CVE-2026-75486
songquanpeng--one-api	one-api gates one of its two channel-pinning paths and not the other. middleware/auth.go permits a request to name a specific channel either through a suffix on the API key or through a URL path parameter. The suffix path is reached	2026-08-26	8.5	CVE-2026-81027

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	only after model.IsAdmin succeeds and otherwise rejects the caller, while the path-parameter branch sets the selected-channel value from c.Param("channelid") with no role check at all. The route carrying that parameter sits behind token authentication only, so any account holding a valid API token reaches it. The value flows to the distributor, which loads the channel by integer identifier with no scoping to the caller's user or group, and then sets the outbound Authorization header to that channel's stored key and directs the request at the channel's base URL. A low-privilege account can therefore pin any channel by incrementing an identifier, causing the server to make upstream requests bearing an operator-configured provider key the account was never granted, and bypassing both the per-group restriction and the channel's model allowlist.			
sonirico--mcp-shell	mcp-shell is an MCP server for running shell commands securely, auditably, and on demand. Prior to 0.6.0, the default Docker security.yaml includes /bin/bash in allowed_executables, while security.go validates only the first token and checkBlockedPatternsAndCommands does not reject the shell command-mode flag -c. A caller of the shell_exec MCP tool can provide the command argument `/bin/bash -c <arbitrary-command>`, which passes validation and reaches executor.go, where parseCommand and exec.CommandContext execute the arbitrary command as mcpuser outside the intended allowlist. This issue is fixed in version 0.6.0.	2026-08-25	8.4	CVE-2026-55581
sonirico--mcp-shell	mcp-shell is an MCP server for running shell commands securely, auditably, and on demand. Prior to 0.6.0, the default security.yaml allows /usr/bin/git, while security.go omits ! from containsShellMetacharacters and containsDangerousShellConstructs and applies no per-executable argument policy. A caller of the shell_exec MCP tool can provide the command argument /usr/bin/git -c alias.pwn=!<arbitrary-command>, causing Git to create a shell alias and execute arbitrary OS commands as the mcp-shell process user. The default Docker image runs as mcpuser with Git installed and secure mode enabled, so the bypass is exploitable in the default deployment without additional authentication beyond MCP connectivity. This issue is fixed in version 0.6.0.	2026-08-25	8.4	CVE-2026-55582
SourceCodester--Simple Online Food Ordering System	A weakness has been identified in SourceCodester Simple Online Food Ordering System 1.0. This vulnerability affects unknown code of the file /fos/admin/ajax.php?action=save_user. This manipulation of the argument Username causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-24	7.3	CVE-2026-78197
SourceCodester--Simple Online Food Ordering System	A security vulnerability has been detected in SourceCodester Simple Online Food Ordering System 1.0. This issue affects some unknown processing of the file /fos/admin/ajax.php?action=add_to_cart. Such manipulation of the argument pid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	2026-08-24	7.3	CVE-2026-78198
SourceCodester--Simple Online Food Ordering System	A vulnerability was detected in SourceCodester Simple Online Food Ordering System 1.0. Impacted is an unknown function of the file /fos/view_prod.php. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2026-08-24	7.3	CVE-2026-78199
SourceCodester--Simple Online Food Ordering System	A vulnerability was found in SourceCodester Simple Online Food Ordering System 1.0. This issue affects some unknown processing of the file /fos/admin/ajax.php?action=confirm_order. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	2026-08-24	7.3	CVE-2026-78247
SourceCodester--Simple Online Food Ordering System	A vulnerability was determined in SourceCodester Simple Online Food Ordering System 1.0. Impacted is an unknown function of the file /fos/admin/ajax.php?action=save_settings. This manipulation of the argument Name causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-24	7.3	CVE-2026-78248
SourceCodester--Simple Online Food Ordering System	A vulnerability has been found in SourceCodester Simple Online Food Ordering System 1.0. This affects an unknown function of the file /admin/ajax.php?action=login2. The manipulation of the argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2026-08-26	7.3	CVE-2026-81203
sparklemotion--nokogiri	Nokogiri before 1.13.2 (CRuby, when using packaged libraries) ships vendored libxml2 2.9.12 and libxslt 1.1.34, which are affected by two upstream CVEs. Via CVE-2021-30560 in libxslt, an application transforming XML with untrusted XSL stylesheets is vulnerable to a denial-of-service attack. Via CVE-2022-23308 in libxml2, an application parsing an untrusted document with parse option	2026-08-25	9.8	CVE-2022-51000

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	DTDVALID set to true and NOENT set to false may be vulnerable to denial of service, memory disclosure, or code execution. Nokogiri 1.13.2 upgrades vendored libxml2 to 2.9.13 and libxslt to 1.1.35.			
sparklemotion--nokogiri	Nokogiri before 1.15.6 and 1.16.x before 1.16.2 (CRuby, when using the packaged libxml2) is affected by a use-after-free vulnerability in libxml2 (CVE-2024-25062) in the xmlTextReader module, which underlies Nokogiri::XML::Reader. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing a crafted XML document can lead to an xmlValidatePopElement use-after-free. Nokogiri 1.15.6 and 1.16.2 resolve this by upgrading the packaged libxml2 to 2.11.7 and 2.12.5 respectively. JRuby and installations using system libxml2 are not affected.	2026-08-25	9.8	CVE-2024-58378
sparklemotion--nokogiri	Nokogiri before 1.18.3 contains a stack buffer overflow vulnerability in libxml2 when reporting DTD validation errors with long QName prefixes, and a use-after-free vulnerability during validation against untrusted XML Schemas. Attackers can trigger these vulnerabilities by providing malicious DTD content or untrusted XSD files to cause denial of service or potential code execution.	2026-08-25	9.8	CVE-2025-71407
sparklemotion--nokogiri	Nokogiri versions before 1.13.5 contain an integer overflow vulnerability in packaged libxml2 buffer handling functions that allows attackers to cause out-of-bounds memory writes. Attackers can exploit this by crafting multi-gigabyte XML files to trigger buffer overflows resulting in information disclosure, data modification, or denial of service.	2026-08-25	8.6	CVE-2022-50999
sparklemotion--nokogiri	Nokogiri before 1.11.4 (CRuby implementation only, when the packaged/vendored libxml2 is used) bundles libxml2 2.9.10, which is affected by multiple vulnerabilities addressed in libxml2 2.9.12, including a memory leak in xmlSchemaValidateStream (CVE-2019-20388), a global buffer over-read in xmlEncodeEntitiesInternal (CVE-2020-24977), a heap-based buffer overflow (CVE-2021-3517), and an out-of-bounds read (CVE-2021-3518). Processing crafted XML documents may lead to denial of service, information disclosure, or memory corruption.	2026-08-25	7.5	CVE-2021-47996
sparklemotion--nokogiri	Nokogiri before 1.13.9 (CRuby implementation using packaged libraries) bundles libxml2 v2.9.14, which is affected by CVE-2022-40304 (data corruption / double-free from an entity reference cycle when entity content is allocated from a dict) and CVE-2022-40303 (integer overflows when parsing with XML_PARSE_HUGE). Nokogiri 1.13.9 upgrades the packaged libxml2 to v2.10.3 to address these issues. Processing crafted XML input may lead to denial of service or memory corruption. (The advisory also references CVE-2022-2309, a NULL pointer dereference via iterwalk/canonicalize, which maintainers determined does not affect Nokogiri users.)	2026-08-25	7.5	CVE-2022-50998
sparklemotion--nokogiri	Nokogiri before 1.14.3 (CRuby implementation only, when using the packaged libxml2) bundles libxml2 v2.10.3, which is vulnerable to NULL pointer dereferences in XML Schema processing (xmlSchemaFixupComplexType, CVE-2023-28484, and xmlSchemaCheckCOSSTDerivedOK). An attacker who supplies a crafted/malformed XML schema can cause libxml2 to dereference a NULL pointer and potentially segfault, resulting in a denial of service. Nokogiri 1.14.3 upgrades the packaged libxml2 to v2.10.4 to resolve these issues.	2026-08-25	7.5	CVE-2023-54354
sparklemotion--nokogiri	Nokogiri before 1.18.4 bundles a vulnerable version of libxslt (prior to 1.1.43) that contains two use-after-free vulnerabilities: CVE-2025-24855 (use-after-free of the XPath context node due to xsltEvalXPathStringNs leaking xpathCtxt->node) and CVE-2024-55549 (use-after-free related to excluded result prefixes/namespaces). Processing crafted XSLT can trigger memory corruption. Nokogiri 1.18.4 upgrades the bundled libxslt to 1.1.43 to resolve these issues.	2026-08-25	7.8	CVE-2025-71406
sparklemotion--nokogiri	Nokogiri versions before 1.19.3 contain regular expression denial of service vulnerabilities in the CSS selector tokenizer affecting string-literal and identifier tokenization. Attackers can inject adversarial CSS selectors into methods like Node#css, Node#at_css, and Searchable#search to cause exponential regex backtracking and denial of service.	2026-08-25	7.5	CVE-2026-79770
speechbrain--speechbrain	SpeechBrain before 1.1.1 contains an arbitrary code execution vulnerability that allows attackers to execute arbitrary code by supplying a crafted CKPT.yaml checkpoint metadata file parsed with PyYAML's unsafe loader during candidate enumeration in Checkpointer.recover_if_possible(). Attackers can embed malicious Python object construction tags such as !!python/object/apply in any CKPT.yaml file within the configured checkpoint path to trigger code execution during candidate discovery, even if the malicious checkpoint is never selected for recovery.	2026-08-27	8.8	CVE-2026-10036

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring AI	Analyzing a PDF with a deeply nested or cyclic table of contents can cause a StackOverflowError in the ingestion thread. Spring AI 2.0.0 Spring AI 1.1.0 - 1.1.8 Spring AI 1.0.0 - 1.0.9	2026-08-26	7.5	CVE-2026-47851
Spring--Spring AI	A local attacker on a multi-user host can pre-create the deterministic cache path and plant a malicious ONNX model file. Spring AI 2.0.0 Spring AI 1.1.0 - 1.1.8 Spring AI 1.0.0 - 1.0.9	2026-08-26	7.5	CVE-2026-47852
Spring--Spring Authorization Server	Spring Authorization Server's default consent page renders user-controlled values without HTML entity encoding. When using the DefaultConsentPage, an attacker can craft an OAuth2 authorization request containing a malicious value that is stored server-side and later rendered unencoded in the default consent page presented to the end user. Spring Authorization Server 1.5.0 - 1.5.8 Spring Authorization Server 1.4.0 - 1.4.11	2026-08-27	8.2	CVE-2026-59316
Spring--Spring Cloud Config	The base directory (spring.cloud.config.server.svn.basedir) used by the Spring Cloud Config Server to clone SVN repositories to is susceptible to time-of-check-time-of-use (TOCTOU) attacks. Spring Cloud Config 5.0.0 - 5.0.4 Spring Cloud Config 4.3.0 - 4.3.4 Spring Cloud Config 4.0.0 - 4.2.8 Spring Cloud Config 3.1.14 and earlier	2026-08-26	7.2	CVE-2026-47836
Spring--Spring Cloud Gateway	Spring Cloud Gateway JsonToGrpcGatewayFilterFactory allows arbitrary Spring Resource locations for defining the proto descriptor. Spring Cloud Gateway 5.0.0 - 5.0.2 Spring Cloud Gateway 4.3.0 - 4.3.5 Spring Cloud Gateway 4.0.0 - 4.2.9 Spring Cloud Gateway 3.1.13 and earlier	2026-08-27	7.7	CVE-2026-47879
Spring--Spring Data REST	Spring Data REST does not guard identifier (@Id) and version (@Version) properties against mutation via RFC 6902 JSON Patch (application/json-patch+json) requests. Spring Data REST 5.1.0 Spring Data REST 5.0.0 - 5.0.6 Spring Data REST 4.5.0 - 4.5.12 Spring Data REST 4.0.0 - 4.4.15 Spring Data REST 3.7.20 and earlier	2026-08-27	7.1	CVE-2026-47849
Spring--Spring Integration	An operator who calls JdbcMessageStore.addAllowedPatterns(...) to restrict deserialization receives no protection at all when the store is a Spring-managed bean. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	2026-08-27	8	CVE-2026-59307
Spring--Spring Integration	When an IntegrationFlow uses .fluxTransform() with an asynchronous/reordering fluxFunction that emits raw payloads, concurrent requests on the same FluxMessageChannel subscription have their reply headers (replyChannel, errorChannel, correlationId, any propagated security/tenant headers) copied from whichever message was most recently consumed upstream. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	2026-08-27	8.2	CVE-2026-59324
Spring--Spring Security	Spring Security's embedded UnboundID LDAP server (UnboundIdContainer) unconditionally registers an administrative credential and binds its listener to all available network interfaces. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 - 6.5.11 Spring Security 6.4.0 - 6.4.18 Spring Security 5.8.0 - 5.8.27 Spring Security 5.7.0 - 5.7.25	2026-08-27	9.4	CVE-2026-59270
Spring--Spring Security	Spring Security Authorization Server's default consent page renders user-controlled values without HTML entity encoding. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6	2026-08-27	8.2	CVE-2026-47877
Spring--Spring Security	Authentication Bypass by Capture-replay vulnerability in Spring Spring Security allows Spring Security's DPoPProofJwtDecoderFactory contains a cache-based replay attack vulnerability. The internal cache storing JWT ID claims has a strict size limit, allowing attackers to evict legitimate entries by flooding the server with dummy requests, then replay intercepted valid DPoP proofs. This issue affects Spring Security: 7.1.0, from 7.0.0 through 7.0.6, and from 6.5.0 through 6.5.11.	2026-08-25	7.4	CVE-2026-41707
Spring--Spring Security	An application using Spring Security's WebAuthn support may be vulnerable to user verification bypass when using a distributed HTTP session store. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 - 6.5.11 Spring Security 6.4.0 - 6.4.18	2026-08-26	7.4	CVE-2026-47841
SpringBlade--SpringBlade	SpringBlade versions from 2.7.3 up to but not including 5.0.0 contain a privilege escalation vulnerability that allows authenticated attackers to create system administrator accounts by sending crafted POST requests to an unprotected internal Feign user-creation endpoint exposed via @RestController without authorization checks. Attackers can exploit the gateway's authentication filter, which only validates JWT parsing without verifying user roles or caller identity, and leverage a hardcoded JWT signing key embedded in publicly available JARs to forge tokens and escalate privileges from a low-privilege user to administrator, enabling cross-tenant data pollution and persistent backdoor access.	2026-08-28	8.1	CVE-2026-56100
stalwartlabs--stalwart	Stalwart Mail Server does not compare an OAuth redirect target against any registered destination in its default configuration. The validation routine in	2026-08-26	8.1	CVE-2026-81036

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	crates/http/src/auth/oauth/registration.rs returns success immediately when the client-authentication requirement is disabled, and that requirement is false in the shipped settings, so the supplied redirect value is neither matched against a registered client nor otherwise constrained. The value is stored with the authorization code, and the login page reads it back and sends the browser to it with the code attached. A request naming a destination the attacker controls therefore delivers a valid authorization code there once the account holder authenticates, and because the token endpoint checks only that the redirect presented at exchange matches the one recorded with the code, the same party can exchange it for access and refresh tokens and read the account's mail.			
StarRocks-- StarRocks	StarRocks performs no privilege check when a legacy synchronous materialized view is dropped. Every other statement type routed through AuthorizerStmtVisitor calls into Authorizer before execution, but visitDropMaterializedViewStatement returns immediately with a comment stating the check happens in execution logic. That holds only for asynchronous materialized views: LocalMetastore.dropMaterializedView calls Authorizer.checkMaterializedViewAction inside a branch taken when the resolved table is a MaterializedView. A legacy synchronous materialized view is stored as a rollup index on an OlapTable rather than a MaterializedView, so the other branch runs, reaching AlterJobMgr.processDropMaterializedView and MaterializedViewHandler, neither of which contains any Authorizer call. The former locates the target by scanning every OlapTable in the named database for a matching rollup index, and the latter validates only table state and name conflicts. Any authenticated account can therefore drop a legacy synchronous materialized view belonging to any database, holding no grant on the view, the base table or the database, and the drop is indistinguishable from an authorized one.	2026-08-26	7.1	CVE-2026-80346
Strategy11-- Formidable Charts	The Formidable Charts plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.0.1 via the 'frm_graph' parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Successful exploitation requires Formidable Forms Lite, Formidable Forms Pro, and Formidable Charts to be active and requires the wp-content/uploads/frm-charts/ directory to exist, normally after an image-format chart is rendered.	2026-08-26	7.5	CVE-2026-15990
strategy11team-- Formidable Forms WordPress Form Builder for Contact Forms, Calculators, Quizzes & More	The Formidable Forms - WordPress Form Builder for Contact Forms, Calculators, Quizzes & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'frm_user_id' parameter in all versions up to, and including, 6.33.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. By forging frm_user_id to match an administrator's user ID - discoverable via the public WordPress REST API - an unauthenticated attacker causes wp_kses_post() to serve as the only output filter, which preserves the injected payload structurally intact; the plugin's admin JavaScript then decodes and executes it automatically on page load.	2026-08-26	7.2	CVE-2026-18331
Stylemix-- MasterStudy LMS	Unauthenticated Arbitrary File Deletion in MasterStudy LMS <= 3.7.42 versions.	2026-08-24	8.6	CVE-2026-78284
sudo-project--sudo	Sudo through 1.9.17p2 fails to apply intercept policy checks to the execveat system call in ptrace-based intercept mode. Users permitted to run specific commands can execute denied programs by calling execveat directly or through fexecve, bypassing policy enforcement and logging.	2026-08-29	7.8	CVE-2026-82474
Super Forms-- Super Forms	Unauthenticated Arbitrary File Download in Super Forms <= 6.3.315 versions.	2026-08-24	7.5	CVE-2026-28167
sveltejs--kit	SvelteKit versions from 2.49.0 through 2.53.2 (fixed in 2.53.3) contain a deserialization expansion issue in the experimental form remote function. When an application enables experimental.remoteFunctions and uses the form function to process the files array without validating files.length or individual file sizes, an attacker can submit relatively small inputs that expand into very large file arrays, leading to expensive processing and denial of service.	2026-08-28	7.5	CVE-2026-82259
sveltejs--kit	SvelteKit (@sveltejs/kit) versions >=2.49.0 and <=2.52.1 with experimental remote functions (experimental.remoteFunctions) and form enabled contain a memory exhaustion vulnerability in remote form deserialization. Malformed form data can cause excessive memory allocation, crashing the server process and resulting in denial of service. Fixed in 2.52.2.	2026-08-28	7.5	CVE-2026-82260
sveltejs--kit	SvelteKit (@sveltejs/kit) versions >=2.49.0 and <=2.52.1 with experimental remote functions and form enabled contain a CPU exhaustion vulnerability in form	2026-08-28	7.5	CVE-2026-82261

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	deserialization. An attacker can send malformed form data to cause the server to become unresponsive while processing the request, resulting in denial of service. Fixed in 2.52.2.			
Synology-- Synology Chat Server	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in extract domain in Synology Chat Server before 2.4.5-22148 allows remote authenticated users, via a UI interaction, to read or write arbitrary files and conduct denial-of-service attacks in DSM.	2026-08-28	9	CVE-2026-40541
TangibleWP-- MyHome Core	The MyHome Core plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 4.4.5. This is due to missing authorization in the send_link() AJAX handler and improper token validation in the activate() function. This makes it possible for unauthenticated attackers to generate an activation token for an unconfirmed user account and obtain a valid authentication cookie for that account, including administrators. Successful exploitation requires the MyHome theme to be configured in legacy/WPBakery mode with frontend registration and confirmation email enabled, and the target account must not already have the myhome_agent_confirmed user meta set.	2026-08-30	9.8	CVE-2026-15980
TarsCloud-- TarsWeb	TarsWeb decides whether a request comes from a trusted local caller using a client-controlled header. app.js sets Koa's proxy option to true without naming which upstream proxies may be trusted and without limiting the number of forwarded hops, so the request address Koa reports is taken from the X-Forwarded-For header supplied by the caller. In middleware/ssoMiddleware.js a single branch covers both the ignored-path list and the ignoreIps allowlist from config/loginConf.js, which contains the loopback address, and that branch assigns the effective account identity from the uid query parameter before falling through to the request without validating any ticket, cookie or password. A request carrying a forged X-Forwarded-For value naming the loopback address and a uid naming an existing account therefore reaches every route the console mounts as that account, including an administrator, with no credential of any kind. Those routes include user and role administration, service configuration, and package upload and deployment. Version 3.0.16 separates the two branches so that a match on the address allowlist assigns the configured default account rather than one named by the caller.	2026-08-26	9.8	CVE-2026-80349
TarsCloud-- TarsWeb	TarsWeb enforces its per-application roles by calling AuthService from individual controller methods, and four methods in app/controller/patch/PatchController.js make no such call. uploadAndPublish accepts a package upload and then builds and dispatches a deployment task to every server matching the supplied application and module name, while its sibling uploadPatchPackage, which only stores the package, does check developer authorization first. The only precondition uploadAndPublish enforces is that the named server is registered, and any registered server in the installation satisfies it. downloadPackage and deletePatchPackage select a package by an unscoped sequential primary key covering every application's uploads, and setPatchPackageDefault changes which package a given application deploys by default. Any authenticated account, including one holding a role scoped to a single unrelated application, can therefore push a package to and trigger its deployment on any server the console manages, retrieve or delete any other application's package, and change which package is deployed by default.	2026-08-26	8.8	CVE-2026-80348
TBTAK BLGEM Software Technologies Research Institute-- Liderahenk	Use of Hard-coded Credentials vulnerability in TÃfÃ“BÃ„Ã°TAK BÃ„Ã°LGEM Software Technologies Research Institute Liderahenk allows Try Common or Default Usernames and Passwords. This issue affects Liderahenk: before 3.5.5.	2026-08-26	9.1	CVE-2026-75896
TBTAK BLGEM Software Technologies Research Institute-- Liderahenk	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') vulnerability in TÃfÃ“BÃ„Ã°TAK BÃ„Ã°LGEM Software Technologies Research Institute Liderahenk allows LDAP Injection. This issue affects Liderahenk: from 3.4.0 before 3.5.5.	2026-08-26	7.5	CVE-2026-19271
team-telnyx-- telnyx-mcp	The Telnyx MCP server exposed its HTTP transport on every interface and did not require a caller credential. packages/mcp-server/src/http.ts served MCP on the root path with a listener bound to all interfaces and parsed the caller's authentication headers in a mode that did not fail when they were absent, so a request without any credential completed initialisation and dispatched tools. Dispatch forwarded the server's own stored credentials, the Telnyx API key and client secret together with the code-execution key, to the upstream endpoint, so	2026-08-27	9.1	CVE-2026-81098

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	an unauthenticated caller able to reach the port acted with them. The current code defaults the host to loopback, requires a server API key, and enforces it in middleware.			
TeamViewer--Full Client	A command injection vulnerability in TeamViewer Full Client and Host for Linux prior to version 15.81.5 allows a remote attacker to execute arbitrary commands in the context of the current user via a specially crafted URL sent through the out-of-session chat feature. Exploitation requires user interaction by clicking the malicious link.	2026-08-26	8.8	CVE-2026-19042
TeamViewer--Full Client, Host, QuickSupport & Portable	Improper neutralization of path traversal sequences in TeamViewer Desktop Clients prior Version 15.81.5 allows an authenticated remote session participant to write files to unintended locations on the local file system via file transfer or virtual file clipboard mechanisms. An attacker can leverage this behavior to achieve arbitrary file write and potentially execute code with the privileges of the affected user.	2026-08-26	7.5	CVE-2026-16444
Tenda--HG10	A weakness has been identified in Tenda HG10 300001138. Affected by this issue is the function formIPv6Routing of the file /boaform/admin/formIPv6Routing of the component Boa Web Server. This manipulation of the argument destNet causes buffer overflow. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-30	10	CVE-2026-82542
thembay--Urna	Unauthenticated Cross Site Scripting (XSS) in Urna <= 2.6.2 versions.	2026-08-24	7.1	CVE-2026-66610
Theme-Rex--FreightCo	Unauthenticated PHP Object Injection in FreightCo <= 1.1.15 versions.	2026-08-24	9.8	CVE-2026-66650
ThemeBing--ProLancer Element	Subscriber SQL Injection in ProLancer Element <= 1.4.8 versions.	2026-08-24	8.5	CVE-2026-32471
ThemeBing--ProLancer Element	Subscriber Broken Access Control in ProLancer Element <= 1.4.8 versions.	2026-08-24	7.1	CVE-2026-28190
themefusion--Avada (Fusion) Builder	The Avada theme for WordPress is vulnerable to Arbitrary File Write in all versions up to, and including, 7.16 when the Fusion Builder plugin is installed and active in versions up to, and including, 3.16. This is due to a chain of authorization and input validation weaknesses across the two components that makes it possible for unauthenticated attackers to write attacker-controlled files to the server. This can be used to create and execute arbitrary PHP files, resulting in remote code execution and complete site compromise. Successful exploitation requires both Avada and Fusion Builder to be installed and active, as well as certain administrator-authored content to be present.	2026-08-26	9.8	CVE-2026-18431
Thinking Software Technology--EFence	EFence developed by Thinking Software Technology has an Arbitrary File Upload vulnerability. Unauthenticated remote attackers can upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	2026-08-26	9.8	CVE-2026-80235
Thinking Software Technology--EFence	EFence developed by Thinking Software Technology has a SQL Injection vulnerability. Unauthenticated remote attackers can access file upload functionality and read database contents.	2026-08-26	8.2	CVE-2026-80236
Thinking Software Technology--EFence	EFence developed by Thinking Software Technology has an Arbitrary File Upload vulnerability. Authenticated remote attackers can upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.	2026-08-26	8.8	CVE-2026-80237
TIM Solutions--TIM Flow	TIM Flow before 26.0.6 contains a CRLF injection vulnerability that allows remote attackers to inject arbitrary HTTP headers and response body content by embedding unsanitized carriage return and line feed sequences in the rt URL parameter, which is reflected into Set-Cookie response headers. Attackers can craft malicious requests to induce authenticated users to execute arbitrary JavaScript in their browser context, enabling session token theft and account credential modification.	2026-08-24	8.1	CVE-2026-39915
tomdever--wpForo Forum	The wpForo Forum plugin for WordPress is vulnerable to SQL Injection via the 'referer' parameter in all versions up to, and including, 2.4.17. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-28	7.5	CVE-2026-5097
tophive--UltimateAI	Subscriber Arbitrary File Upload in UltimateAI <= 3.1.0 versions.	2026-08-24	9.9	CVE-2026-32559
TOTOLINK--A720R	A vulnerability was determined in TOTOLINK A720R 4.1.5cu.630_B20250509. This impacts the function setMacFilterRules of the file cstecgi.cgi of the component MAC Filtering. Executing a manipulation of the argument desc can lead to memory corruption. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-30	9.1	CVE-2026-82539

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
TOTOLINK--N600R	A security vulnerability has been detected in TOTOLINK N600R 4.3.0cu.7647_B20210106. The affected element is the function setSystemConfig of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument Hostname leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	2026-08-25	10	CVE-2026-79911
TOTOLINK--N600R	A vulnerability was detected in TOTOLINK N600R 4.3.0cu.7647_B20210106. The impacted element is the function getCurrentTime of the file /cgi-bin/cstecgi.cgi. Performing a manipulation of the argument ntp_server results in command injection. The attack can be initiated remotely. The exploit is now public and may be used.	2026-08-25	8.3	CVE-2026-79912
TriliumNext--Trilium	Trilium is an open-source hierarchical note-taking application. In versions prior to 0.104.0, the automatic image-download feature accepts file:// URLs in a note's img tags and reads the referenced local file with no path validation, allowing any authenticated user to disclose arbitrary files readable by the Trilium process. When a text note is saved, Trilium scans its HTML for image sources and downloads each external one; because the HTML sanitizer keeps file as an allowed scheme, a source such as file:///etc/passwd is passed straight to a filesystem read and its contents are stored as a note attachment the user can then retrieve. Pointing the same primitive at an unbounded source such as /dev/zero causes uncontrolled memory allocation that crashes the server process. The feature is enabled by default and is reachable through the web UI, the ETAPI, the web clipper, and note imports, requiring only an authenticated session or an ETAPI token. This issue is fixed in version 0.104.0	2026-08-27	8.1	CVE-2026-53580
TriliumNext--Trilium	Trilium is an open-source hierarchical note-taking application. In versions up to and including 0.103.0, the public share-search endpoint does not enforce the per-note shareCredentials and shareHiddenFromTree controls, allowing an unauthenticated visitor to read the titles, tree paths, and content of protected shared notes. The endpoint authorizes only the ancestor note supplied in the request and then runs a full-text search across the entire published subtree, returning each matching note's title, share identifier, and hierarchical path without re-checking whether that individual note requires a share password or is hidden from the navigation tree. Because the search matches note content, an attacker can enumerate protected notes and use the endpoint as a boolean oracle that confirms arbitrary substrings, recovering the full contents of notes that should be gated behind a password. This issue is fixed in version 0.104.0.	2026-08-27	7.5	CVE-2026-77438
TRtek Technological Products Computer Software Hardware Industry and Trade Limited Company--Software Repository Management	Unrestricted upload of file with dangerous type vulnerability in TRtek Technological Products Computer Software Hardware Industry and Trade Limited Company Software Repository Management allows Upload a Web Shell to a Web Server. This issue affects Software Repository Management: before 2fb4acee.	2026-08-25	9.8	CVE-2026-16286
TrustedFirmware--Trusted Firmware-M	On the Trusted Firmware-M (TF-M) 2 through 2.3.0 platform before 00d1b3e, mailbox initialization on PSOC64 and RP2350 accepts a non-secure, unvalidated, supplied pointer.	2026-08-26	7	CVE-2026-54467
Tutor LMS--Tutor LMS	The Tutor LMS WordPress plugin before 4.0.6 does not prevent request data from overwriting internal variables while rendering templates, allowing unauthenticated users to invoke arbitrary zero-argument PHP functions and receive their output.	2026-08-27	9.8	CVE-2026-19092
tw93--Pake	Pake before 3.13.1 joins the JavaScript-supplied filename for the download_file Tauri command onto the user's Downloads directory with no sanitization. A filename containing path traversal sequences (for example ../Library/LaunchAgents/com.evil.plist) or an absolute path resolves outside ~/Downloads. The command then fetches attacker-controlled content from the supplied URL (via Rust HTTP, not the browser) and writes it to that path. A script that can invoke the command can overwrite user-writable files and install persistence (macOS LaunchAgents, Linux autostart, Windows Startup), leading to code execution in the user account. All desktop apps generated from an affected Pake tree expose the same command.	2026-08-30	8.8	CVE-2026-82635

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
typeorm--typeorm	TypeORM's SelectQueryBuilder.distinctOn accepts an array of strings and stores it on the expression map without validation. For PostgreSQL-family drivers, createSelectDistinctExpression in src/query-builder/SelectQueryBuilder.ts joins that array and interpolates the result into the generated statement as SELECT DISTINCT ON (values), with no escaping, quoting, identifier validation or allowlist, and without routing the values through replacePropertyNames or the driver's escape helper. Because the interpolation point is a parenthesized SQL expression list rather than an identifier-only position, a supplied element may carry arbitrary expressions, including correlated subqueries. An application that forwards a client-controlled value into distinctOn, for instance to let a caller choose a deduplication column, allows that client to read data anywhere the application's database role can reach through boolean or time-based inference, independently of the entity being queried. validateOrderByCondition, the allowlist check guarding the orderBy family in the same class, is not applied to this path.	2026-08-24	7.5	CVE-2026-76848
Ubiquiti Inc--EdgeMAX EdgeSwitch	A malicious actor with access to an adjacent network could exploit a Buffer Overflow vulnerability found in a DHCPv6-enabled EdgeMAX EdgeSwitch to initiate a Remote Code Execution on such device.	2026-08-26	9.6	CVE-2026-77532
Ubiquiti Inc--UID Enterprise Agent	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UID Enterprise Agent to execute a Command Injection on the host device.	2026-08-26	9.1	CVE-2026-77542
Ubiquiti Inc--UniFi Access Application	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.	2026-08-26	9.9	CVE-2026-77543
Ubiquiti Inc--UniFi Access Application	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.	2026-08-26	9.9	CVE-2026-77546
Ubiquiti Inc--UniFi Access Application	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.	2026-08-26	9.9	CVE-2026-77547
Ubiquiti Inc--UniFi Access Application	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in UniFi Access Application to escalate privileges on the host device.	2026-08-26	9.9	CVE-2026-77553
Ubiquiti Inc--UniFi Connect Application	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Connect Application to escalate privileges within the UniFi Connect Application.	2026-08-26	8.2	CVE-2026-77538
Ubiquiti Inc--UniFi Connect Display Cast Pro	A malicious actor with access to the network and under certain conditions could exploit an Improper Access Control vulnerability found in UniFi Connect Display Cast Pro to escalate privileges on the device.	2026-08-26	9	CVE-2026-77551
Ubiquiti Inc--UniFi Enterprise Audio/Video Bridge	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Enterprise Audio/Video Bridge to execute a Command Injection on the device.	2026-08-26	9.8	CVE-2026-77552
Ubiquiti Inc--UniFi Network Application	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UniFi Network Application to execute a Command Injection on an adopted device.	2026-08-26	9.1	CVE-2026-77535
Ubiquiti Inc--UniFi Network Application	A malicious actor with access to the network and high privileges could exploit an Improper Access Control vulnerability found in UniFi Network Application to escalate privileges within the UniFi Network Application.	2026-08-26	9.1	CVE-2026-77541
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network could exploit an Improper Neutralization of CRLF Sequences vulnerability found in certain devices running UniFi OS to bypass authentication to such UniFi OS devices or instances.	2026-08-26	10	CVE-2026-77550
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in certain devices running UniFi OS to escalate privileges within such UniFi OS devices or instances.	2026-08-26	9.9	CVE-2026-77534
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in certain devices running UniFi OS to escalate privileges within such UniFi OS devices or instances.	2026-08-26	9.9	CVE-2026-77536
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UniFi OS Server to execute a Command Injection on the host device.	2026-08-26	9.1	CVE-2026-77539
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network and high privileges could exploit an Improper Input Validation vulnerability found in UniFi OS Server to execute a Command Injection on the host device.	2026-08-26	9.1	CVE-2026-77540

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network, low privileges and under certain conditions could exploit an Active Debug Code vulnerability found in certain devices running UniFi OS to escalate privileges within such UniFi OS devices or instances.	2026-08-26	9	CVE-2026-77545
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network and under certain conditions could exploit an Improper Neutralization of CRLF Sequences vulnerability found in certain devices running UniFi OS to bypass authentication to such UniFi OS devices or instances.	2026-08-26	9	CVE-2026-77549
Ubiquiti Inc--UniFi Protect AI Key	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Protect AI Key to escalate privileges on the device.	2026-08-26	9.8	CVE-2026-77557
Ubiquiti Inc--UniFi Protect Application	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Protect Application to execute a Command Injection on the host device.	2026-08-26	10	CVE-2026-77537
Ubiquiti Inc--UniFi Protect Application	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Protect Application to execute a Command Injection on the host device.	2026-08-26	9.9	CVE-2026-77533
Ubiquiti Inc--UniFi Protect Application	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Protect Application to execute a Command Injection on the host device.	2026-08-26	9.9	CVE-2026-77548
Ubiquiti Inc--UniFi Talk Application	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Talk Application to execute a Command Injection on the host device.	2026-08-26	10	CVE-2026-77554
UnitedOver, LLC--Digits	Unauthenticated Privilege Escalation in Digits <= 9.2 versions.	2026-08-24	9.8	CVE-2026-28165
Unitree Robotics--G1 EDU	Unitree G1 EDU firmware through 1.5.2 contains an unauthenticated remote code execution vulnerability that allows network-adjacent attackers to execute arbitrary commands as root by chaining three weaknesses: an unauthenticated WebRTC-to-DDS bridge on TCP port 9991, a static AES-128 key stored with world-readable permissions, and a path traversal flaw in the chat_go knowledge upload API. Attackers can publish DDS control messages to restart the bashrunner service, plant a malicious payload in its script execution directory via path traversal, and trigger execution of that payload as uid 0 through the bashrunner shell subprocess.	2026-08-27	8.8	CVE-2026-76639
Unitree Robotics--G1 EDU	Unitree G1 EDU firmware through 1.5.2 contains multiple chained vulnerabilities in the BLE GATT server and WiFi provisioning stack that allow unauthenticated proximate attackers to achieve root code execution without pairing or credentials by exploiting an unquoted heredoc variable in the WiFi provisioning script and a buffer overflow in the SSID chunk accumulator. Attackers can send crafted BLE writes to overflow a fixed BSS buffer across BLE connections, corrupting an adjacent mainloop function pointer dispatch entry that is subsequently invoked by the cleanup path passing attacker-controlled data to system() as uid 0.	2026-08-27	7.5	CVE-2026-76640
UTT--HiPER 1200GW	A flaw has been found in UTT HiPER 1200GW up to 2.5.3-170306. Affected is the function strcpy of the file /goform/formConfigFastDirectionW. Executing a manipulation of the argument ssid can lead to buffer overflow. The attack may be performed from remote. The exploit has been published and may be used.	2026-08-24	8.8	CVE-2026-78170
UTT--HiPER 1250GW	A vulnerability was detected in UTT HiPER 1250GW up to 3.2.7-210907-180535. This impacts the function strcpy of the file /goform/aspRemoteApConfTempSend of the component HTTP Request Handler. Performing a manipulation of the argument Profile results in stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2026-08-24	9.9	CVE-2026-78169
vanquish--WooCommerce File Approval	Unauthenticated Arbitrary File Deletion in WooCommerce File Approval <= 10.7 versions.	2026-08-24	8.6	CVE-2026-28171
vastsa--FileCodeBox	A vulnerability was detected in vastsa FileCodeBox up to 2.3. This vulnerability affects the function update_file_usage of the file apps/base/views.py of the component Pickup Limit Handler. Performing a manipulation results in race condition. It is possible to initiate the attack remotely. The exploit is now public and may be used. Upgrading to version 2.5.0 is able to resolve this issue. The patch is named 8d7d856c62d73badd0797eb4daec8d2ff10a403a. Upgrading the affected component is recommended.	2026-08-30	7.3	CVE-2026-82543
vesoft-inc--nebula	NebulaGraph exposes its runtime configuration over an unauthenticated HTTP service. Each daemon starts the web service defined in src/web/service/WebService.cpp, whose bind address defaults to all interfaces, and registers routes for reading and writing gflags alongside status and statistics.	2026-08-26	9.8	CVE-2026-81032

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Neither the service nor its router carries any authentication, token check or address restriction. The read route returns the daemon's full set of runtime flag values, which includes the configured certificate, key and certificate-authority paths, the password file path, data directories and the transport-security enable flags. The write route parses a supplied map and applies each entry through the gflags runtime setter, so a caller able to reach the port can change the daemon's behaviour without restarting it, including disabling the transport-security flags, redirecting log files and altering flags such as failed_login_attempts and password_lock_time_in_secs. Public reports of this endpoint describe a single name, enable_authorize, being refused by the handler; at release 3.8.0 that refusal is not present and the handler applies every name it is given.			
VillaTheme--Suggestion Engine for WooCommerce	Contributor SQL Injection in Suggestion Engine for WooCommerce <= 2.0.11 versions.	2026-08-27	8.5	CVE-2026-81277
VillaTheme--WPBulky	Contributor SQL Injection in WPBulky <= 1.2.2 versions.	2026-08-28	8.5	CVE-2026-82227
VMware by Broadcom--Spring Security (OAuth2 Authorization Server module)	In versions of Spring Security's OAuth2 Authorization Server module 7.0.0 through 7.0.4, when Dynamic Client Registration is explicitly enabled, the registration endpoint performs insufficient validation of certain client metadata fields supplied by the registering client. An attacker who possesses a valid Initial Access Token can register a malicious client with crafted metadata, which, depending on server configuration and how the metadata is later rendered or used, may result in Stored Cross-Site Scripting (XSS), Privilege Escalation, or Server-Side Request Forgery (SSRF).	2026-08-27	9.6	CVE-2026-59354
VoltAgent--voltagent	VoltAgent through 2.1.20 fails to validate conversation ownership in memory API handlers, allowing authenticated users to access other users' conversations. Attackers can read, modify, and delete arbitrary conversations and messages by supplying caller-controlled identifiers to memory endpoints.	2026-08-28	8.1	CVE-2026-82283
voxel51--fiftyone	FiftyOne renders a dataset field's description as markup. The sidebar field-information component at app/packages/core/src/components/FieldLabelAndInfo/index.tsx passes the description string to React's dangerouslySetInnerHTML, and no layer between storage and render escapes or sanitises it; the neighbouring info values in the same component are rendered as React children and are escaped, so the description is the only raw path. A description is free-form text held in the dataset schema, so it persists in the database and travels with an exported or published dataset. Opening a dataset obtained from another party and hovering the field runs the stored markup in the application's origin. That origin is shared with the FiftyOne server, whose media route returns the contents of a caller-named absolute path and which is unauthenticated in the open-source server, so the injected script can read local files and reach the dataset and operator endpoints as the viewing user.	2026-08-26	7.1	CVE-2026-80426
vrana--adminer	Adminer before 5.4.3 fails to sanitize the server field before constructing a PDO DSN string, allowing unauthenticated attackers to inject ODBC parameters via semicolons. Attackers can inject TraceFile and TraceOn parameters to write PHP code to the web root, achieving remote code execution when the trace file is accessed.	2026-08-25	9.8	CVE-2026-56705
vrana--adminer	Adminer before 5.4.3 contains an arbitrary file deletion vulnerability in SQLite mode where the database-list drop action fails to validate file extensions before deletion. An authenticated attacker can submit arbitrary relative file paths in the db[] parameter to delete any files writable by the PHP process.	2026-08-25	8.1	CVE-2026-34968
vrana--adminer	Adminer versions before 5.4.3 contain an unrestricted file upload vulnerability in the AdminerFileUpload plugin that allows authenticated users to upload PHP files by exploiting a permissive default extension allowlist. Attackers can upload PHP webshells to columns ending in _path and execute arbitrary code as the web-server user when uploadPath is web-served.	2026-08-25	8.8	CVE-2026-56702
vrana--adminer	Adminer before 5.4.3 contains a remote code execution vulnerability in SQLite query handling where VACUUM INTO is not blocked despite ATTACH restrictions. Authenticated attackers can execute VACUUM INTO to write PHP code to arbitrary file paths and execute commands on the server.	2026-08-25	7.2	CVE-2026-56703
warmcat--libwebsockets	A vulnerability was found in warmcat libwebsockets 4.5.0. Impacted is the function report_raw_cbor of the file lib/misc/lecp.c of the component LECP CBOR Recording. The manipulation results in out-of-bounds write. The attack can be launched remotely. The exploit has been made public and could be used. The patch	2026-08-24	7.3	CVE-2026-78161

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is identified as 1d44554a1bb262db63ff4e240152a9deecd99054. It is best practice to apply a patch to resolve this issue.			
wazuh--wazuh	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.4.0 through 4.14.6, a party holding the cluster key can write, overwrite, or delete arbitrary files under /var/ossec on worker nodes, leading to remote code execution as root. During cluster file synchronization, the non-merged branch of update_master_files_in_worker() moves each staged file to a destination derived only from safe_join(), which confines the path to /var/ossec but never verifies that the file lands in the directory declared by its cluster_item_key. Because the destination check present on the primary node and on the worker's merged branch was not applied, a peer can place files at attacker-chosen locations under /var/ossec, including paths that are executed as root, and the delete branch has the same gap. This is an incomplete fix for CVE-2026-30893, which addressed traversal outside /var/ossec but left this path able to redirect files anywhere within it. This issue is fixed in version 4.14.7.	2026-08-27	9.1	CVE-2026-61800
wazuh--wazuh	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. The ip-customblock active response script contains a path traversal vulnerability that lets an attacker create or delete arbitrary files on the filesystem as root. The script builds a file path by concatenating the srcip field taken from alert JSON directly onto the fixed /ipblock/ base directory, without validating that the value is a well-formed IP address. Because the extraction routine returns the raw string unchecked, an attacker who can trigger alert-matching log events with a crafted srcip containing ../ sequences can escape the base directory. The block action opens the resulting path in append mode, creating an empty file at an arbitrary location, while the unblock action passes it to remove(), deleting an arbitrary file; since the active response daemon runs as root, this includes sensitive files such as system credentials and Wazuh configuration. Unlike the sibling scripts host-deny.c, default-firewall-drop.c, and firewall-drop.c, which reject non-IP input via get_ip_version(), ip-customblock.c omits this validation. This issue is fixed in version 4.14.7.	2026-08-27	8.1	CVE-2026-54083
wazuh--wazuh	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.2.0 through 4.14.6, multiple active response scripts pass attacker-influenced alert fields to privileged system commands without validating their format, allowing argument injection into tools that run as root. Five of the eight scripts that handle the srcip field, route-null.c, netsh.c, pf.c, npf.c, and ipfw.c, omit the get_ip_version() check that rejects non-IP input, and disable-account.c passes the dstuser field to passwd/chuser with only a comparison against "root". An attacker who can inject crafted log events, for example via syslog, can supply srcip or dstuser values that, when an active response rule triggers, are passed unvalidated to firewall and account-management commands such as pfctl, npfctl, ipfw, route, netsh, and passwd. This enables injecting additional command arguments, and on Windows the unquoted CreateProcess command-line concatenation in wopenv() lets a srcip containing spaces add further arguments, while disable-account.c can be abused to lock arbitrary system accounts. This issue is fixed in version 4.14.7.	2026-08-27	7.1	CVE-2026-54085
WBW--WooBeWoo Product Filter Pro	Unauthenticated SQL Injection in WooBeWoo Product Filter Pro <= 3.1.8 versions.	2026-08-24	9.3	CVE-2026-32554
WebKit--WebKit	A flaw was found in WebKitGTK. Processing malicious web content can cause a use-after-free issue due to improper memory handling and result in memory corruption.	2026-08-24	8.8	CVE-2026-78376
Webkul--QloApps	Webkul QloApps does not perform proper validation on uploaded file extensions or MIME types before moving the file to a publicly accessible directory. A remote, authenticated attacker with administrative privileges could upload executable files and achieve remote code execution. Fixed in 153ec1c.	2026-08-25	7.2	CVE-2026-75496
Webkul--QloApps	Webkul QloApps does not validate request parameters before a database query. A remote, authenticated attacker with administrative privileges could send a crafted SQL query to the 'bo_query' parameter in the 'CustomerMessage.php' file. Fixed in 123c97c.	2026-08-25	7.2	CVE-2026-75497
Webkul--QloApps	Webkul QloApps does not validate request parameters before a database query. A remote, authenticated attacker with administrative privileges could send a crafted SQL query to the 'bo_query' parameter in the 'Address.php' file. Fixed in 123c97c.	2026-08-25	7.2	CVE-2026-75498

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WeblateOrg--weblate	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, the REST API did not properly enforce the scope of project- and workspace-scoped teams, allowing a user to submit invalid team configurations through the API. By assigning projects to a team via these unvalidated requests, a user could grant access to projects they were not authorized to see or manage. This could expose private projects and permit translation, repository, and project-management operations outside the user's intended permission scope. This issue is fixed in version 2026.7.	2026-08-26	8.1	CVE-2026-55228
WeblateOrg--weblate	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, a project administrator can read files outside their repository through the App store metadata download feature, which resolves attacker-influenced paths without adequately confining them to the repository. This is an incomplete fix for CVE-2026-34242, whose original patch failed to fully prevent the path traversal, allowing the arbitrary file read to persist. A user with project-administrator privileges can therefore disclose the contents of files on the Weblate host that lie outside the project's repository. This issue is fixed in version 2026.7.	2026-08-26	7.7	CVE-2026-61792
webpack--webpack-dev-middleware	webpack-dev-middleware resolves a request to a local file in getFilenameFromUrl by testing the request pathname against a traversal guard and then slicing it at a fixed character offset. The guard, UP_PATH_REGEXP applied to path.normalize(`./\${pathname}`), only matches "." that stands as a whole path segment, while the containment test is the string comparison pathname.startsWith(publicPathPathname) and the file path is built as path.join(outputPath, pathname.slice(publicPathPathname.length)). When the configured publicPath has no trailing slash, a request such as GET /assets../.env against publicPath /assets yields the pathname /assets../.env, whose only dot-dot sits inside the segment "assets.." and so passes the guard, but the offset slice cuts within that segment and hands "../.env" to path.join, resolving one directory above outputPath. Reading a file from that path requires the middleware to be backed by the physical filesystem, which happens when writeToDisk is true or a custom outputFileSystem is supplied, since the default memfs volume holds only build output. Traversal depth is limited to a single directory because a separately delimited dot-dot segment is collapsed during URL parsing before the guard runs. The default publicPath value of "auto" resolves to "/" and is not affected. This is an incomplete fix for CVE-2024-29180: the guard and offset slice were introduced by that fix and are present in every release from 5.3.4, 6.1.2 and 7.1.0 onward.	2026-08-24	7.4	CVE-2026-76844
weDevs Pte. Ltd--WP Project Manager Pro	Subscriber SQL Injection in WP Project Manager Pro <= 4.0.1 versions.	2026-08-24	8.5	CVE-2026-32478
wedevs--ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce	The ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce plugin for WordPress is vulnerable to Unrestricted File Type Upload in all versions up to, and including, 1.17.8 via the save_attachments() function. This is due to missing file extension validation and missing path normalization when CRM Email Connect processes inbound IMAP email attachments. This makes it possible for unauthenticated attackers to send a crafted email to the site's configured inbound mailbox with a forged References header matching the plugin's expected pattern and an attachment filename such as `../helper.php`, causing the cron-based IMAP sync job to write attacker-controlled PHP outside of the .htaccess-protected `crm-attachments` directory and into `wp-content/uploads/`. On configurations where PHP executes in uploads, this can lead to remote code execution. Exploitation requires the CRM module and IMAP Email Connect feature to be enabled and configured.	2026-08-26	9.8	CVE-2026-18080
weDevs--WP Project Manager	Unauthenticated PHP Object Injection in WP Project Manager <= 4.0.6 versions.	2026-08-24	9.8	CVE-2026-78262
Weidmueller Interface--IE-SR-2TX-WL	The web-based management interface uses a modified uhttpd server with CGI shell scripts. The HTTP Basic Authentication username, taken directly from the Authorization header without sanitization, is inserted into a shell command string executed via the system() function. By submitting a specially crafted username containing shell metacharacters, an unauthenticated attacker with network access to the device can escape the command context and execute arbitrary commands with root privileges.	2026-08-25	9.8	CVE-2026-63586
Weidmueller Interface--IE-SR-2TX-WL-4G-EU	The SMS control function of IE-SR-2TX-WL-4G devices can require a password for SMS commands via the 'Enable Password Authorization' setting. The device increments a retry counter on each failed SMS password attempt; after 5	2026-08-25	8.6	CVE-2026-63587

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	consecutive failed attempts, SMS password authorization is automatically disabled. An unauthenticated remote attacker who is able to send SMS messages to the device can deliberately trigger this by submitting 5 or more invalid passwords, after which subsequent SMS commands are executed without requiring a password, resulting in potential limited configuration tampering, limited information leakage and potentially full loss of availability.			
Weptile--Mobile App for WooCommerce	Unauthenticated Broken Access Control in Mobile App for WooCommerce <= 0.4.62 versions.	2026-08-27	8.6	CVE-2026-27330
wibu-systems-ag--codemeter-runtime	If CodeMeter Runtime before 8.41a or 9.10 is configured as a server, the configuration command handler does not enforce network- origin restrictions. Commands intended only for local or same-network clients can therefore be executed by arbitrary remote peers. An attacker can read potentially sensitive configuration data and overwrite selected values in Server.ini. This does include the hash of the credentials for the CodeMeter WebAdmin, enabling WebAdmin takeover.	2026-08-27	8.6	CVE-2026-81573
wibu-systems-ag--codemeter-runtime	In CodeMeter Runtime before versions 8.41a and 9.10, the logger does not sanitize input strings in certain cases, allowing an attacker to inject printf-style format specifiers. This can be used to reliably crash CodeMeter and disclose sensitive information such as process memory and stack canaries. The attack works locally, for example by using cmu --set-proxy to set the proxy value, and remotely when combined with CVE-2026-81573 by setting General.ProxyServer and then triggering this vulnerability.	2026-08-27	8.2	CVE-2026-81574
wibu-systems-ag--codemeter-runtime	In CodeMeter Runtime from version 8.40 to (excluding) 8.41a and 9.00 to (excluding) 9.10, cmu.exe --create-io --file C: creates a predictable temporary file under C:\CM-Stick. The directory and file paths are not properly checked for NTFS reparse points, such as junctions or symbolic links, before file operations are performed. A local attacker can create a junction at the temporary file that points to an arbitrary system path. Because CodeMeter Runtime runs with System privileges, this could allow arbitrary files to be deleted with System privileges and potentially enable local privilege escalation.	2026-08-27	7.8	CVE-2026-81572
wibu-systems-ag--codemeter-runtime	If configured as a server, CodeMeter Runtime before versions 8.41a and 9.10 accepts requests with opcode 0x5e, which contain the data length and the data itself. Missing bounds checking on the data length value can lead to out of bounds reads, causing a segmentation fault that ultimately crashes the CodeMeter Runtime.	2026-08-27	7.5	CVE-2026-81575
wibu-systems-ag--codemeter-runtime	If configured as a server, CodeMeter Runtime before versions 8.41a and 9.10 issues handles per connection and relies on a cryptographically weak SID as sole authenticator. An attacker can brute-force the SID, recover another session's handle number, and read license information belonging to another handle.	2026-08-27	7.7	CVE-2026-81576
wibu-systems-ag--wibukey	In WibuKey for Windows before version 6.71, an untrusted pointer dereference in the WibuKey2_64.sys kernel driver for 64-bit Windows allows an attacker to exploit a write-what-where primitive, enabling local privilege escalation. This can be leveraged to execute arbitrary code, run an administrator shell, or gain full control over the system.	2026-08-27	8.8	CVE-2026-81579
wibu-systems-ag--wibukey	Improper validation of memory boundaries in WibuKey64.sys of WibuKey up to 6.70 for Windows can be exploited by an attacker by setting the pointers outside the scope of the program. This usually results in a denial of service, yet we cannot rule out the possibility of exploits that can cause Remote Code Execution and Privilege Escalation (since the driver runs with system privileges).	2026-08-27	8.8	CVE-2026-81581
wintercms--winter	Winter is a free, open-source content management system (CMS) based on the Laravel PHP framework. Prior to 1.2.13, custom CSS supplied through the Brand Settings Styles field by a backend user with the backend.manage_branding permission is compiled by the LESS parser and rendered without sanitization on every backend page, allowing stored cross-site scripting against backend users. This issue is fixed in version 1.2.13.	2026-08-26	8.1	CVE-2026-32257
wintercms--winter	Winter is a free, open-source content management system (CMS) based on the Laravel PHP framework. From 1.2.10 through 1.2.12, authenticated backend users with the backend.manage_editor permission can store custom Markup Styles that are compiled by the LESS parser and rendered without sanitization on every backend page, allowing stored cross-site scripting. This issue is fixed in version 1.2.13.	2026-08-26	8.1	CVE-2026-32258
wintercms--winter	Winter CMS versions before 1.2.13 contain an incomplete fix for a Twig sandbox escape vulnerability in System\ Twig\ SecurityPolicy that allows authenticated	2026-08-25	8.4	CVE-2026-79774

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	backend users with template-editing permissions to bypass sandbox restrictions. Attackers can exploit method forwarding through Eloquent models and query builders using methods like saveQuietly(), deleteQuietly(), increment(), decrement(), and newQuery() to read and modify arbitrary database records, execute arbitrary SQL, and achieve remote code execution by injecting PHP into template code sections.			
wolfSSL Inc.-- wolfEngine	wolfEngine before 1.4.1 generates the 8-byte explicit AES-GCM nonce once when the TLS write key is set and never increments it per record. As a result every TLS 1.2 and DTLS 1.2 AES-GCM record within a connection is encrypted under an identical key and nonce pair. Reusing a GCM key and nonce discloses the keystream (the XOR of two ciphertexts equals the XOR of their plaintexts, so one known record recovers the others) and leaks the GHASH authentication key, enabling authentication tag forgery. AES-CCM, TLS 1.3, and non-TLS use of the cipher are not affected.	2026-08-28	7.4	CVE-2026-81020
wolfSSL Inc.-- wolfProvider	wolfProvider before 1.2.2 generates the 8-byte explicit AES-GCM nonce once when the TLS write key is set and never increments it per record. As a result every TLS 1.2 and DTLS 1.2 AES-GCM record within a connection is encrypted under an identical key and nonce pair. Reusing a GCM key and nonce discloses the keystream (the XOR of two ciphertexts equals the XOR of their plaintexts, so one known record recovers the others) and leaks the GHASH authentication key, enabling authentication tag forgery. AES-CCM, TLS 1.3, and non-TLS use of the cipher are not affected.	2026-08-28	7.4	CVE-2026-81019
WP Fastest Cache-- WP Fastest Cache	The WP Fastest Cache WordPress plugin before 1.5.1 does not validate the Host header before using it to build the URLs of the asset files it embeds in the pages it caches, and does not include that header in the cache key, allowing unauthenticated attackers to poison cached pages with references to a server they control and have arbitrary JavaScript run for every subsequent visitor.	2026-08-25	7.5	CVE-2026-74932
WP Legal Pages-- WPLegalPages	Unauthenticated Broken Authentication in WPLegalPages <= 3.7.0 versions.	2026-08-24	7.3	CVE-2026-78259
WP Manage Ninja-- Fluent Boards Pro	Editor Arbitrary File Upload in Fluent Boards Pro <= 2.0.11 versions.	2026-08-27	9.1	CVE-2026-78274
WP Manage Ninja-- Fluent Boards Pro	Editor PHP Object Injection in Fluent Boards Pro <= 2.0.11 versions.	2026-08-27	7.2	CVE-2026-78276
WP Manage Ninja-- FluentBooking Pro	Unauthenticated Cross Site Request Forgery (CSRF) in FluentBooking Pro <= 2.2.4 versions.	2026-08-27	8.1	CVE-2026-81273
WP Manage Ninja-- FluentCRM Pro	Editor Privilege Escalation in FluentCRM Pro <= 3.1.12 versions.	2026-08-27	7.2	CVE-2026-78271
WP ManageNinja LLC--FluentCRM Pro	Author SQL Injection in FluentCRM Pro <= 3.1.12 versions.	2026-08-24	7.6	CVE-2026-78270
WP Media--WP Rocket	The WP Rocket plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 3.21.0.1. This is due to insufficient input sanitization and output escaping of user-supplied data via the rocket_beacon AJAX endpoint. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-28	7.2	CVE-2026-5934
WPCafe--WP Cafe Pro	Unauthenticated Local File Inclusion in WP Cafe Pro < 3.0.15 versions.	2026-08-24	9.8	CVE-2026-66587
WPCafe--WP Cafe Pro	Unauthenticated Sensitive Data Exposure in WP Cafe Pro < 3.0.15 versions.	2026-08-24	7.5	CVE-2026-66585
WPDeveloper-- NotificationX Pro	The NotificationX Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 3.1.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-25	7.2	CVE-2026-78563
wpgenie-- WooCommerce Lottery	The WooCommerce Lottery plugin for WordPress is vulnerable to Time-Based SQL Injection via 'orderby' and 'order' GET Parameters in all versions up to, and including, 2.2.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-26	7.5	CVE-2026-18884
WPMU DEV-- Smush Image Compression and Optimization	Unauthenticated Denial of Service Attack in Smush Image Compression and Optimization <= 4.2.0 versions.	2026-08-28	7.5	CVE-2026-81285

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Radio Field (Save and Continue Draft) in all versions up to, and including, 1.57.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is exploitable because the Save-and-Continue draft submission AJAX endpoint is registered as nopriv, allowing unauthenticated attackers to bypass radio field option-membership validation and persist a crafted payload that, when rendered on the Submissions admin page, is auto-executed via the bundled Inputmask library's data-attribute callback binding.	2026-08-25	7.2	CVE-2026-18323
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Rich-Text Textarea Field in all versions up to, and including, 1.57.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires that the targeted Textarea field has the Rich-Text editor option enabled.	2026-08-28	7.2	CVE-2026-18324
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to DOM-Based Reflected Cross-Site Scripting via the 'error_description' parameter in all versions up to, and including, 1.57.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability is only triggerable on pages hosting a Forminator form configured to use the Stripe Checkout Sessions payment API, which became the default in 1.56.0.	2026-08-25	7.2	CVE-2026-18328
wpmudev--WPMU DEV Dashboard	The WPMU DEV Dashboard plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 5.0.1. This is due to inconsistent and ambiguous HMAC message construction between the unauthenticated 'wdpsso_step1' and 'wdpsso_step2' AJAX actions, where step 1 signs and discloses an unseparated concatenation of the token, state, redirect, and domain values, while step 2 verifies an unseparated concatenation that omits the domain field. This makes it possible for unauthenticated attackers, on sites connected to WPMU DEV with Hub SSO enabled and mapped to an administrator, to obtain a valid HMAC from step 1 and replay it to step 2 by moving the domain value into the redirect field, resulting in an authenticated administrator session.	2026-08-28	9.8	CVE-2026-76581
WWBN--AVideo	AVideo (current commit e01e41ecc and earlier) exposes stream credentials through the plugin/Live/view/Live_restreams/getLiveKey.json.php endpoint. Supplying a 'token' request parameter waives both the Live::canRestream() access gate and the restream ownership check, causing the endpoint to return any restream's stream_key and stream_url (credentials for external platforms such as YouTube, Facebook, and Twitch) without authentication. The token is merely encryptString() of an integer id with no user binding, expiry, or authentication tag. Because encryption uses AES-256-CBC with a deterministic IV and no MAC, and because intval() accepts any string beginning with a digit, an unauthenticated attacker can forge valid tokens using the public encryption oracle in view/url2Embed.json.php, disclosing arbitrary users' stream credentials.	2026-08-30	8.6	CVE-2026-82645
WWBN--AVideo	AVideo before 24.0 contains a server-side request forgery vulnerability in the isSSRFSafeURL function that fails to extract embedded IPv4 addresses from NAT64, 6to4, and Teredo IPv6 transition address formats. Unauthenticated attackers can bypass SSRF protections via the LiveLinks proxy endpoint to reach internal services and cloud metadata endpoints by encoding private IPv4 targets in transition address formats.	2026-08-27	7.5	CVE-2026-81678
WWBN--AVideo	WWBN AVideo (current e01e41ecc and earlier) contains a brute-force rate limiting bypass in enforceRateLimit(), which protects login.json.php and 13 other endpoints. The function stores its attempt counter via a cache layer (ObjectYPT::setCacheGlobal) that silently discards writes for any client identified as a bot by isBot(). Because isBot() treats a missing User-Agent header as a bot by default - and also matches common bot identifiers such as 'curl', 'bot', 'crawler', and 'spider' - the counter never increments for such clients, so the rate limit never fires. An unauthenticated attacker can therefore submit unlimited login attempts (e.g., by omitting the User-Agent header or using curl's default User-Agent), enabling unrestricted password-guessing attacks.	2026-08-30	7.5	CVE-2026-82644
WWBN--AVideo	WWBN AVideo contains a server-side request forgery filter bypass vulnerability in the isSSRFSafeURL function that fails to normalize NAT64 addresses written in	2026-08-30	7.1	CVE-2026-82648

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	hexadecimal form. Attackers can bypass SSRF protections by supplying hex-encoded NAT64 addresses like 64:ff9b::a9fe:a9fe to reach cloud metadata services and loopback interfaces.			
Xiiiozet--Xiiiozet LK100W	Xiiiozet LK100Wt contains an authentication weakness within an administrative service that may allow an attacker to bypass intended access controls and obtain command execution capabilities. Successful exploitation could allow unauthorized interaction with privileged functionality and may lead to complete device compromise.	2026-08-27	9.8	CVE-2026-76943
Xiiiozet--Xiiiozet LK100W	Xiiiozet LK100W exposes a critical management function that can be invoked without authentication, allowing a remote attacker to enable administrative services that should be restricted. Successful exploitation may permit unauthorized access to the device.	2026-08-27	9.8	CVE-2026-78239
Xiiiozet--Xiiiozet LK100W	Xiiiozet LK100W is vulnerable to OS command injection through its web-based management interface. An authenticated attacker may be able to execute arbitrary operating system commands with elevated privileges, potentially resulting in unauthorized access to sensitive information or complete device compromise.	2026-08-27	8.8	CVE-2026-78037
xorbisai--inference	Xinference loads models with Hugging Face remote code execution unconditionally enabled, and before version 2.12.0 exposes no setting to disable it. Six loader call sites pass trust_remote_code=True as a literal or as an unconditional default: RerankModel._get_tokenizer in xinference/model/rerank/core.py, SentenceTransformerRerankModel.load in xinference/model/rerank/sentence_transformers/core.py, SentenceTransformerEmbeddingModel.load in xinference/model/embedding/sentence_transformers/core.py, FlagEmbeddingModel.load in xinference/model/embedding/flag/core.py, and two sites in xinference/model/llm/transformers/core.py where PytorchModel._sanitize_model_config and PytorchModel._get_components default the value to True. Because a caller with model launch access can register a model whose type is unknown and supply an arbitrary model path, the server reaches _auto_detect_type and then AutoTokenizer.from_pretrained, which imports and executes Python declared by the model directory's own tokenizer_config.json auto_map, running attacker-supplied code with the privileges of the worker process. Version 2.12.0 gates every site behind allow_trust_remote_code and the XINFERENCE_TRUST_REMOTE_CODE setting, permitting remote code only for bundled built-in models.	2026-08-24	8.8	CVE-2026-76841
yalla ya!--Simple Payment	Unauthenticated Broken Access Control in Simple Payment <= 2.5.2 versions.	2026-08-28	7.5	CVE-2026-81767
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs allows a user with SystemPrivilege.ControlArchiving to create a double-quoted StreamSQL column name that is interpolated into generated Java source by Expression.fillCode_InputDefVars and Expression.sanitizeName. A sum aggregate reaches yamcs-core/src/main/java/org/yamcs/yarch/streamsql/CompilableAggregateExpression.java and yamcs-core/src/main/java/org/yamcs/yarch/streamsql/funct/SumExpression.java through SelectExpression.compile, where Janino SimpleCompiler.cook compiles the injected source. POST /api/archive/{instance}:executeSql can therefore execute arbitrary Java in the Yamcs server process, exposing mission data and credentials and permitting telemetry tampering or denial of service. This issue is fixed in versions 5.12.8 and 5.13.2.	2026-08-28	9.1	CVE-2026-55511
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs inserts templateArgs from POST /api/instances and PATCH /api/instances/{instance} into YAML through VarStatement.append in yamcs-core/src/main/java/org/yamcs/templating/VarStatement.java without YAML-context escaping. The rendered configuration is parsed by YamcsServer.createInstance and loaded by YamcsServerInstance, allowing an attacker to inject a services entry for org.yamcs.ProcessRunner. Deployments without security.yaml expose the operation through the guest superuser, while secured deployments require SystemPrivilege.CreateInstance. Successful exploitation executes commands as the Yamcs service account. This issue is fixed in versions 5.12.8 and 5.13.2.	2026-08-28	9.8	CVE-2026-55559
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs LikeExpression.fillCode_getValueReturn in yamcs-core/src/main/java/org/yamcs/yarch/streamsql/LikeExpression.java inserts an	2026-08-28	9.9	CVE-2026-55565

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unescape LIKE pattern into Java source compiled by Expression.getCompiledExpression through SimpleCompiler.cook instead of applying ValueExpression.escapeJavaString. The pattern can originate from POST /api/archive/{instance}:executeSql, POST /api/archive/{instance}:streamSql, POST /api/archive/{instance}/tables/{table}:readRows, GET /api/archive/{instance}/events, or activity searches, including paths available with ReadTables, ReadEvents, or ReadActivities. A quote in the pattern can inject Java that runs as the Yamcs server process. This issue is fixed in versions 5.12.8 and 5.13.2.			
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs omits authorization checks in IndexesApi.listPacketIndex, IndexesApi.listEventIndex, Cop1Api.disable, Cop1Api.resume, Cop1Api.initialize, Cop1Api.updateConfig, and TimeApi.setTime. An authenticated low-privilege user can read packet and event index metadata without ObjectPrivilegeType.ReadPacket, alter COP-1 link state without SystemPrivilege.ControlLinks, and manipulate simulation time. These operations can disclose telemetry metadata, disrupt telecommand handling, and affect system integrity and availability. This issue is fixed in versions 5.12.8 and 5.13.2.	2026-08-28	8.8	CVE-2026-55521
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.11.13, Yamcs StaticFileHandler.locateFile resolves an unauthenticated request path without using Path.normalize and Path.toAbsolutePath to confirm that the absolute path remains within the configured staticRoots. A path containing traversal segments can escape the intended web root and return an arbitrary readable host file. The flaw is in yamcs-core/src/main/java/org/yamcs/http/StaticFileHandler.java and can disclose sensitive operating-system and application data. This issue is fixed in version 5.11.13, and the 5.12 line is fixed from version 5.12.0.	2026-08-28	7.5	CVE-2026-55552
Zbtlink--L3_V2_8	Zbtlink L3_V2_8 firmware 3.0.0.4.528, Zbtlink WE826-T2 firmware 19.1101, Zbtlink ZBT-7628 firmware 1.0.0.2.007, Zbtlink ZBT-ZBT7621 firmware 1.0.0.3.001, MoreQuick MQAC-7620, MQAC-7620A, MQAP-7620, MQAP-7620A, and MQAP-7628 firmware 1.0.0.2.000, AP522 firmware 1.0.0.2.014, AP7628 and HC5661A firmware 3.0.0.4.380, APG721B firmware 19.0809, HK300 firmware 1.0.0.2.032, and MAP-N10 firmware 1.0.0.2.044 ship a backdoor command-and-control implant (yunmgrd) reachable over an unauthenticated cleartext UDP channel to a hardcoded C2 server. A remote unauthenticated attacker on the network path can hijack the channel and execute arbitrary commands as root. The attacker can also modify DNS entries, exfiltrate PPPoE credentials, and open reverse SSH tunnels.	2026-08-27	9.8	CVE-2026-74232
Zbtlink--WE1326	Zbtlink WE1326, WE357, WE5926, WE5926-WD, WE826-Q, WE826-T2, WE826-WD, WG108, and WG3526 firmware 19.1101, Zbtlink WE2426-C firmware 19.1112, Zbtlink WE5926-EC_QP firmware 20.0516, Zbtlink WF3526-P firmware 19.051, CTN720-W1, LF-1541, and MT7620N firmware 19.1101, and WRC1 firmware 20.0622 contain an unauthenticated command injection in the infosrvd service (UDP/9992). A remote unauthenticated attacker can send a crafted UDP packet to execute arbitrary commands as root. The service's authentication uses a hardcoded salt and an all-zero wildcard MAC bypass, rendering it ineffective.	2026-08-27	9.8	CVE-2026-74233
zephyrproject--zephyr	The OCPP 1.6 client in subsys/net/lib/ocpp/ocpp_j.c contains a stack buffer overflow in parse_getconfig_msg(). When handling a GetConfiguration request from the central system, the handler copied the attacker-controlled JSON "key" string into the caller's fixed 50-byte stack buffer (skey[CISTR50], declared in subsys/net/lib/ocpp/ocpp.c) using an unbounded strcpy(). The parsed key value points directly into the receive buffer, so its length is bounded only by the message size (CONFIG_OCPP_RECV_BUFFER_SIZE, default 2048). The GetConfiguration message is delivered over the WebSocket connection that the charge point opens to its configured central system. The reader thread ocpp_wsreader() reads the message into ui->recv_buf and dispatches it to parse_getconfig_msg() via the PDU function table. An attacker who controls the central system endpoint, or a man-in-the-middle on an unencrypted connection, can send a GetConfiguration request whose "key" field exceeds 50 bytes and overflow the reader thread's stack with attacker-chosen bytes. The consequence is a remotely triggerable stack smash on the OCPP reader thread: at minimum a denial of service, and plausibly remote code execution depending on build-time hardening such as stack canaries and MPU configuration. The fix replaces the strcpy() with a bounded strncpy(key, payload.key[0], CISTR50 - 1) followed by explicit NUL termination, matching the bounded copies already used by the sibling handlers.	2026-08-25	9.8	CVE-2026-13214

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zephyrproject--zephyr	The Zephyr virtio driver does not validate the descriptor-chain head id that the virtio device writes into the used ring. In virtio_isr() (drivers/virtio/virtio_common.c), the device-written vq->used->ring[idx].id is used directly as an index into vq->recv_cbs[] and vq->desc[], which are both allocated with exactly vq->num entries. recv_cbs[] holds {cb, opaque} callback entries, and the indexed callback pointer is then invoked as cbe.cb(cbe.opaque, used_len). Because the id is consumed as a 16-bit value with no bound check, a malicious or compromised virtio backend (an untrusted hypervisor, or an untrusted hardware/peer-processor virtio device on a PCI or MMIO transport) can supply an id far beyond vq->num. This causes an out-of-bounds read of a {function pointer, argument} pair from heap memory beyond recv_cbs[], after which the driver calls that attacker-shaped pointer in the guest's interrupt context. No guest privileges or user interaction are required; the backend triggers it by writing the shared used ring and raising the queue interrupt. The result is an arbitrary / attacker-influenced function-pointer call in the Zephyr guest, i.e. a control-flow-hijack primitive that can lead to code execution or, at minimum, a reliable crash. The fix rejects any used-ring id >= vq->num before indexing recv_cbs[]/desc[] or invoking the callback. This affects builds using CONFIG_VIRTIO with the PCI or MMIO transport.	2026-08-24	8.8	CVE-2026-13212
Zoneminder--Zoneminder	An authenticated OS command injection vulnerability exists in ZoneMinder's event export functionality. The exportFile HTTP request parameter is passed unsanitized into a shell command executed via PHP's exec(), allowing any authenticated user with View Events permission to execute arbitrary operating system commands on the server.	2026-08-27	8.8	CVE-2026-76060
Zscaler--Client Connector	An authentication bypass issue exists in communications between affected versions of the Zscaler Client Connector and the Zscaler Client Connector Portal.	2026-08-24	9.1	CVE-2026-59564
Zscaler--Client Connector	Multiple vulnerabilities on affected versions of Zscaler Client Connector allow remote code execution, giving an unauthenticated, unprivileged user the ability to execute arbitrary code in the ZCC context.	2026-08-24	9.1	CVE-2026-59568
Zscaler--Client Connector	A remotely exploitable buffer overflow bug can cause a local and kernel denial-of-service attack on affected versions of Zscaler Client Connector on Windows.	2026-08-24	8.8	CVE-2026-59565
Zscaler--Client Connector	A locally exploitable buffer overflow bug can cause a local denial-of-service attack on affected versions of Zscaler Client Connector on Android and ChromeOS.	2026-08-24	8.4	CVE-2026-59566
Zscaler--Client Connector	Multiple vulnerabilities on affected versions of Zscaler Client Connector allow local privilege escalation, giving an unprivileged user the ability to execute arbitrary code in a privileged context.	2026-08-24	8.8	CVE-2026-59567

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
299ko--299Ko	299Ko's public contact form (plugin/contact/controllers/ContactController.php, home()) sets raw POST field values (name, firstname, email, message) into the page template with no sanitization. The template engine's variable output function (common/Template.php, _show_var()) echoes values with no htmlspecialchars() call, and the sink template (contact.tpl) outputs these values unescaped into an HTML attribute and a textarea. An unauthenticated attacker can submit a payload such as name="<script>alert(document.domain)</script>" to achieve reflected XSS against any visitor who submits or is tricked into auto-submitting the form, including a targeted administrator, enabling session token theft.	2026-08-05	6.1	CVE-2026-71249
2wstechnologies--Askeet Talk to Your WooCommerce Data	The Askeet plugin for WordPress is vulnerable to SQL Injection via the 'sql_query' parameter in multiple AJAX actions (askeet_execute_sql_query, askeet_export_all_results) in all versions up to, and including, 3.0. This is due to the askeet_is_safe_query() filter being bypassable using MySQL conditional comments (e.g., /*!UNION*/). The filter strips regular block comments before checking for forbidden SQL keywords, but MySQL interprets conditional comments as executable code. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-05	4.9	CVE-2026-5651
3CORESec--Trapdoor	A weakness has been identified in 3CORESec Trapdoor up to 1.2.2. Affected by this vulnerability is the function DefaultFunction. This manipulation causes improper access controls. The attack can be initiated remotely. The vendor was contacted early about this disclosure.	2026-08-09	6.3	CVE-2026-19358
aaronsb--memory-graph	A vulnerability was detected in aaronsb memory-graph up to 5cfd2382778837b9f6399080956eee670d00452c. Affected by this vulnerability is the function JsonMemoryStorage.createDomain/JsonMemoryStorage.getMemories/JsonMemoryStorage.saveMemories of the file src/tools/memoryTools.ts. The manipulation results in path traversal. The attack must be initiated from a local position. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	5.3	CVE-2026-19285
abdullah1854--MCPGateway	A vulnerability was identified in abdullah1854 MCPGateway up to 549f494a9e363f40530149de324b8097de424230. This impacts the function getUsageByDateRange of the file src/services/claude-usage.ts of the component Claude Usage Range Endpoint. The manipulation of the argument since leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	6.3	CVE-2026-19268
abracadabra50--claude-sesh	A flaw has been found in abracadabra50 claude-sesh 1.0.0. This issue affects the function getEnrichedData/enrichSession of the file src/services/enricher.ts. Executing a manipulation of the argument sessionId can lead to path traversal. The attack needs to be launched locally. This patch is called 786c9d74800e6d0858b65778f31beb71b3983a50. Applying a patch is advised to resolve this issue.	2026-08-09	5.3	CVE-2026-19327
abrinsmead--mindpilot-mcp	A flaw has been found in abrinsmead mindpilot-mcp 0.5.0. Affected by this issue is some unknown functionality of the component HistoryService. This manipulation of the argument ID causes path traversal. The attack needs to be launched locally. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	5.3	CVE-2026-19287

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adenot--mcp-google-search	A vulnerability was determined in adenot mcp-google-search up to 0.3.1. Impacted is an unknown function of the file src/index.ts of the component read_webpage. Executing a manipulation of the argument url can lead to server-side request forgery. The attack is restricted to local execution. This patch is called f071d491b685011ca04e8ab8d586fc65f86bcee1. It is advisable to implement a patch to correct this issue.	2026-08-09	5.3	CVE-2026-19337
Admidio--admidio	Admidio versions before 5.0.11 contain a reflected cross-site scripting vulnerability in the SSO/SAML endpoint that echoes unencoded exception messages to the HTTP response. Unauthenticated attackers can inject arbitrary JavaScript through SAML Issuer elements or LightSaml library parameters to execute code in users' browsers and hijack sessions.	2026-08-03	6.5	CVE-2026-69092
Admidio--admidio	Admidio before 5.0.11 fails to validate target organization membership in role handlers, allowing authenticated role administrators to delete, activate, deactivate, or edit roles belonging to other organizations. Attackers can supply a role UUID from another organization to groups_roles.php handlers to modify that organization's roles without authorization.	2026-08-03	4.9	CVE-2026-69090
Admidio--admidio	Admidio before 5.0.11 does not validate the adm_csrf_token in modules/category-report/preferences.php, which performs persistent Category Report configuration changes based on GET parameters (delete and copy). An attacker can trick an authenticated administrator into visiting a crafted URL to delete or duplicate Category Report configurations, affecting the integrity and availability of that module's configuration.	2026-08-03	4.6	CVE-2026-69093
Admidio--admidio	Admidio before 5.0.11 contains an insecure direct object reference vulnerability in the save_temporary mode of mylist_function.php that allows authenticated users to hijack list configurations. Attackers can enumerate global list UUIDs and overwrite admin-curated global lists or other users' private lists by supplying a list_uuid parameter, transferring ownership and demoting global lists to personal configurations.	2026-08-03	4.3	CVE-2026-69094
Adobe--Adobe Genuine Software Integrity Service	Adobe Genuine Software Integrity Service was affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could have leveraged this vulnerability to bypass security measures and gain unauthorized limited write access. Exploitation of this issue did not require user interaction, but required the attacker to have access to the local environment the application is installed on.	2026-08-07	4	CVE-2026-71381
adolfosalasgomez3011--slidev-builder-mcp	A security flaw has been discovered in adolfosalasgomez3011 slidev-builder-mcp 2.1.0. This affects the function generateChart of the file src/tools/generateAssets.ts of the component generateAssets Tool. Performing a manipulation of the argument outputDir results in command injection. The attack is only possible with local access. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	5.3	CVE-2026-19281
afthemes--WP Post Author Author Box, Multiple Authors, Guest Authors & Custom Avatars	The WP Post Author - Author Box, Multiple Authors, Guest Authors & Custom Avatars plugin for WordPress is vulnerable to generic SQL Injection via the 'wpma_metabox_authors_list' parameter in all versions up to, and including, 3.9.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation is a two-step chain: an attacker first saves a crafted guest-author token via the wpma_metabox_authors_list parameter during post creation or editing, then triggers the injection when any admin user loads the post list screen at /wp-admin/edit.php, causing the injected SQL result to be rendered in the Authors column.	2026-08-05	6.5	CVE-2026-11977

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aizuda--SnailJob (snail-job)	SnailJob 1.7.0 contains a denial of service vulnerability in the FuryUtil.deserialize helper that allows authenticated attackers to crash the server by supplying a crafted Zstandard-compressed payload with an inflated frame_content_size field in the frame header. Attackers can store a base64-encoded Zstandard payload declaring an arbitrarily large decompressed size in a retry task argument, causing the JVM to attempt an unbounded array allocation and triggering an unrecoverable java.lang.OutOfMemoryError when the task is dispatched through the retry-task pipeline.	2026-08-04	6.5	CVE-2026-69702
akaunting--akaunting	Akaunting's shared download route (app/Http/Controllers/Common/Uploads.php::download(), reachable at uploads/{id}/download behind only generic auth middleware) fetched the requested Media record by ID with no verification that it belonged to the requesting portal customer's own company, allowing any authenticated portal customer to download any other company's uploaded files by guessing or enumerating media IDs. Fixed in commit 80ef6d3 (2026-07-12), which added an explicit ownership check comparing the media's parent record contact_id against the requesting user's own contact.	2026-08-05	6.5	CVE-2026-71251
Akshay Menariya--Export Import Menus	Unauthenticated Sensitive Data Exposure in Export Import Menus <= 1.9.2 versions.	2026-08-06	5.3	CVE-2026-66684
aktsmm--skill-ninja-mcp-server	A vulnerability has been found in aktsmm skill-ninja-mcp-server 0.1.0. Impacted is the function getInstalledSkills/installSkill/updateAgentsMd/uninstallSkill of the file src/installer.ts. The manipulation of the argument workspacePath leads to path traversal. The attack needs to be performed locally. Upgrading to version 0.1.1 is recommended to address this issue. The identifier of the patch is 855b46739e0f6e8388f17f9d0066ac4298a3965d. Upgrading the affected component is recommended.	2026-08-09	5.3	CVE-2026-19328
Alex--Featured Video Plus	Unauthenticated Sensitive Data Exposure in Featured Video Plus <= 2.3.3 versions.	2026-08-06	5.3	CVE-2026-66685
aliyun--alibabacloud-dataworks-mcp-server	A security flaw has been discovered in aliyun alibabacloud-dataworks-mcp-server up to 1.0.43. The impacted element is the function ReadResourceRequestSchema of the file src/resources/initResources.ts. The manipulation of the argument request.params.uri results in server-side request forgery. The attack may be launched remotely. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	6.3	CVE-2026-19339
alphawolf--Simple Yearly Archive	The Simple Yearly Archive plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `posttype` attribute of the `SimpleYearlyArchive` shortcode in all versions up to, and including, 2.2.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-05	6.4	CVE-2026-7441
andreahaku--codex_mcp	A vulnerability was found in andreahaku codex_mcp up to 1ff521cc6cc57cfe56ddef946c644b8534771390. The affected element is an unknown function of the file src/codex-process-simple.ts of the component ask MCP Tool. The manipulation of the argument model results in command injection. The attack requires a local approach. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19329
andreahaku--llm_memory_mcp	A weakness has been identified in andreahaku llm_memory_mcp up to f11dc8bcff3ff8cf943a2945f99ff3b0bdc8a6d0. This impacts the function auto.capture of the file src/autolearn/GitHooksManager.ts of the component llm_memory_mcp. Executing a manipulation of the argument hash can lead to	2026-08-08	5.3	CVE-2026-19282

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	command injection. The attack is restricted to local execution. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.			
angrisky56--advanced-reasoning-mcp	A vulnerability was determined in angrisky56 advanced-reasoning-mcp 1.0.0. The impacted element is the function create_system_json/create_library to get_system_json/switch_memory_library of the file src/index.ts. This manipulation causes path traversal. The attack requires local access. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19330
antoineh--Football Pool	The Football Pool plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the `shouttext` POST parameter of the Shoutbox widget in all versions up to, and including, 2.13.4 due to insufficient input sanitization and output escaping. When a shoutbox form submission fails the nonce check (or `shouttext` is empty, or the user is unable to save), the raw POST value is echoed back into a `<textarea>` element using `printf('%s', ...)` with no HTML escaping. This makes it possible for unauthenticated attackers to execute arbitrary web scripts in the browser of an authenticated victim (Subscriber-level or higher) who is tricked into submitting a crafted POST request to a page that contains the Shoutbox widget.	2026-08-05	6.1	CVE-2026-8790
anubissbe--ProjectHub-Mcp	A weakness has been identified in anubissbe ProjectHub-Mcp up to 5.0.0. This affects an unknown function of the file backend-fix/complete_backend.js of the component Webhooks API. This manipulation of the argument url causes server-side request forgery. Remote exploitation of the attack is possible. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	6.3	CVE-2026-19340
Arraytics--WP Event SOLUTION	Unauthenticated Broken Authentication in WP Event SOLUTION <= 4.1.9 versions.	2026-08-06	6.5	CVE-2026-66451
astralisone--rive-mcp-server-core	A vulnerability has been found in astralisone rive-mcp-server-core up to db1d0cc4cd52589116360428b7504fd0ca748b3e. This affects an unknown part of the file packages/mcp-server/src/tools/importRiveFile.ts of the component importRiveFile Flow. Such manipulation of the argument libraryId leads to path traversal. The attack needs to be performed locally. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	5.3	CVE-2026-19288
ATN-B1--CPDLC	Unnumbered Disconnect (U DISC) and malformed Aviation Very High Frequency Link Control frames can terminate sessions and lead to a loss of CPDLC functions requiring a reversion to voice communication and increased controller workload. This type of attack can be carried out remotely over radio frequency.	2026-08-07	5.3	CVE-2025-71410
ATN-B1--CPDLC	Broadcast control frames can disconnect multiple aircraft simultaneously leading to delayed clearances and air traffic controller overload. This type of attack can be carried out remotely over radio frequency.	2026-08-07	5.3	CVE-2025-71411
ATN-B1--CPDLC	Malformed or out-of-sequence frames at the Aviation Very High Frequency Link Control X.25 layers cause repeated resets which may result in increased workload and reduced situational awareness. This type of attack can be carried out remotely over radio frequency.	2026-08-07	5.3	CVE-2025-71413
Autodesk--Revit	A maliciously crafted TIF file, when parsed through certain Autodesk products during image import, can cause an Out-of-Bounds Read in the image handling library. A malicious actor can leverage this vulnerability to cause a denial of service	2026-08-06	5.5	CVE-2026-7405
automateyournetwork--MCPyATS	A vulnerability was identified in automateyournetwork MCPyATS up to 0.1.4. The affected element is the function processGenerateRequest of the file mcp_servers/mermaid/index.ts of the component generate_mermaid_markdown.	2026-08-09	5.3	CVE-2026-19338

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The manipulation of the argument folder/name leads to path traversal. The attack must be carried out locally.			
AWS--amazon-mq-mcp-server	Improper restriction of intended endpoints in the RabbitMQ broker connection tools of the Amazon MQ MCP Server (awslabs.amazon-mq-mcp-server) before 2.0.24 may allow a remote unauthenticated actor (via prompt injection) to obtain Amazon MQ for RabbitMQ broker credentials or OAuth access tokens sent to a crafted endpoint controlled through a broker hostname introduced in the MCP client context. To remediate this issue, users should upgrade to version 2.0.24.	2026-08-03	6.5	CVE-2026-18655
AWS--aws-cli	Key exchange without entity authentication in the EMR SSH helper commands in Amazon AWS CLI before 1.45.28 and AWS CLI v2 before 2.35.3 might allow man-in-the-middle attackers to intercept SSHsessions and file transfers via network positioning between the client and the EMR cluster endpoint. To remediate this issue, users should upgrade to AWS CLI v1 1.45.28 or later, or AWS CLI v2 2.35.3 or later.	2026-08-03	6.8	CVE-2026-18654
AWS--documentdb-mcp-server	Incorrect authorization in the aggregation pipeline tool in Amazon AWS Labs DocumentDB MCP Server before 1.0.12 might allow an authenticated MCP client to perform inappropriate write operations on the connected database via write-capable aggregation pipeline stages that bypass the read-only mode enforcement logic. To remediate this issue, users should upgrade to version 1.0.12 or later.	2026-08-05	5.5	CVE-2026-18954
azer--react-analyzer-mcp	A security flaw has been discovered in azer react-analyzer-mcp up to 335f2a3585f265e2e88352b59b10d3b478d678b0. Affected by this vulnerability is the function generateProjectDocs of the file src/index.ts of the component analyze-projec. The manipulation of the argument projectName results in path traversal. The attack is only possible with local access. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19323
bartekke8it56w2--new-mcp	A vulnerability was determined in bartekke8it56w2 new-mcp 0.1.0. This impacts the function fs.writeFileSync/fs.existsSync/fs.readFileSync of the file index.ts of the component geminithinking. This manipulation of the argument sessionCommand/sessionPath causes path traversal. The attack requires local access. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19370
Baserow--Baserow	A vulnerability was identified in Baserow up to 2.3.2. Affected by this vulnerability is the function verify of the file backend/src/baserow/api/two_factor_auth/views.py of the component 2FA Verify Endpoint. Such manipulation leads to improper authentication. The attack may be launched remotely. This attack is characterized by high complexity. The exploitation appears to be difficult. Upgrading to version 2.3.3 addresses this issue. You should upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-08-04	5	CVE-2026-18816
bazylhorsey--obsidian-mcp-server	A vulnerability was identified in bazylhorsey obsidian-mcp-server 1.0.0. This affects the function readCanvas/writeCanvas of the file src/services/CanvasService.ts. Such manipulation leads to path traversal. An attack has to be approached locally. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19331
bdthemes--Element Pack Addons for Elementor Elementor Widgets,	The Element Pack Addons for Elementor plugin for WordPress is vulnerable to Email Header Injection in all versions up to, and including, 8.3.15 via the `element_pack_contact_form` AJAX action. This is due to insufficient sanitization of newline characters in user-supplied input that gets concatenated into email headers. This makes it possible for unauthenticated attackers to inject arbitrary email headers into emails sent by the contact form.	2026-08-06	5.3	CVE-2026-0673

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elementor Templates, Elementor Addons				
bdthemes-- Element Pack Elementor Addons	Unauthenticated Bypass Vulnerability in Element Pack Elementor Addons <= 8.7.13 versions.	2026-08-06	5.3	CVE-2026-65502
bdthemes-- Ultimate Store Kit Elementor Addons	Unauthenticated Broken Access Control in Ultimate Store Kit Elementor Addons <= 3.0.5 versions.	2026-08-06	6.5	CVE-2026-25403
beardev-- JoomSport for Sports: Team & League, Football, Hockey & more	The JoomSport - for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to time-based SQL Injection via the 'order' parameter in all versions up to, and including, 5.7.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The affected admin page lacks nonce or CSRF protection on the GET request, meaning an unauthenticated attacker could exploit this vulnerability by tricking an authenticated administrator into issuing a crafted request. Additionally, the vulnerability is only triggered when the 'orderby' parameter is also present and non-empty alongside the 'order' parameter.	2026-08-05	4.9	CVE-2026-11920
Bilin Software and Informatics Consultancy Inc.-- HUMANIST Digital Human Resources	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Path Traversal. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	6.5	CVE-2026-14194
Bilin Software and Informatics Consultancy Inc.-- HUMANIST Digital Human Resources	Insufficient session expiration vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Reusing Session IDs (aka Session Replay). This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	6.5	CVE-2026-14465
Bilin Software and Informatics Consultancy Inc.-- HUMANIST Digital Human Resources	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Stored XSS. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	5.4	CVE-2026-14192
Bilin Software and Informatics Consultancy Inc.-- HUMANIST Digital Human Resources	Observable response discrepancy vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Account Footprinting. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	5.3	CVE-2026-14202
Bilin Software and Informatics Consultancy Inc.-- HUMANIST Digital Human Resources	URL redirection to untrusted site ('open redirect') vulnerability in Bilin Software and Informatics Consultancy Inc. HUMANIST Digital Human Resources allows Phishing. This issue affects HUMANIST Digital Human Resources: from 26.0 before 26.1.	2026-08-04	5.4	CVE-2026-14219
Blix--Email Blue Mail Calendar App	A vulnerability was detected in Blix Email Blue Mail Calendar App 2.2.305. Impacted is the function FileDirectory.getDataColumn/FileDirectory.getFileFromUri of the component react-native-receive-sharing-intent. The manipulation of the argument _display_name results in path traversal. The attack is only possible with local access. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	5.3	CVE-2026-18648

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
BoldGrid--W3 Total Cache	Unauthenticated Path Traversal in W3 Total Cache <= 2.10.2 versions.	2026-08-06	6.5	CVE-2026-66695
boringproxy--boringproxy	boringproxy through 0.10.0 contains a resource exhaustion vulnerability that allows any authenticated user to permanently exhaust server file descriptors, goroutines, and memory by sending requests to the GET /loading endpoint with attacker-supplied id query parameter values. Because the handler performs no map-lookup validity check and receives on a nil channel that blocks forever, with no timeout, no context cancellation, and no server-side reclamation due to absent HTTP server timeouts, each malicious request permanently holds one goroutine, one file descriptor, and approximately 50 kB of memory until the server's file descriptor limit is reached and listener Accept calls fail, halting all tunnel traffic forwarding for all users.	2026-08-05	6.5	CVE-2026-70616
Brainstorm Force--Ultimate Addons for Elementor	Contributor Cross Site Scripting (XSS) in Ultimate Addons for Elementor <= 1.45.2 versions.	2026-08-06	6.5	CVE-2026-66688
cemtan--sar2html	A vulnerability was detected in cemtan sar2html 4.0.0. This affects an unknown part of the file sar2html.py of the component Search. Performing a manipulation of the argument Search results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	6.3	CVE-2026-18719
chetans9--core-php-admin-panel	A flaw has been found in chetans9 core-php-admin-panel up to 90d07ed5aac5e0f09b6a5828d7bb2eb83010763f. This issue affects some unknown processing of the file /Applications/MAMP/htdocs/core-php-admin-panel-master/customers.php. Executing a manipulation of the argument filter_col can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	6.3	CVE-2026-18766
chirpstack--chirpstack	ChirpStack's SQLite-backend device tag filtering (chirpstack/src/storage/device.rs, in both get_count() and list()) interpolates the user-supplied tag KEY directly into a raw SQL fragment via Rust's format!() macro ('dsl::sql::<Bool>(&format!("{}", k)).bind::<Text, _>(v)'), while only the tag VALUE is safely parameter-bound via Diesel's .bind(). An authenticated user with device-list access can inject SQL via a crafted tag key when the SQLite backend (chirpstack-sqlite package) is in use; the PostgreSQL backend is unaffected as it uses Diesel's native JSONB containment operator instead of raw SQL string formatting.	2026-08-05	6.5	CVE-2026-71282
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the web-based management interface of Cisco Catalyst SD-WAN Manager could allow an authenticated, remote attacker to view sensitive information in clear text on an affected system. This vulnerability is due to insufficient access control enforcement for specific template types that are not included in the encryption allowlist. A low-privileged attacker could exploit this vulnerability by viewing logs on the local system or on a remote logging server. A successful exploit could allow the attacker to view sensitive authentication credentials, which could lead to further compromise of network infrastructure and connected services.	2026-08-05	6.5	CVE-2026-20294
Cisco--Cisco Enterprise NFV Infrastructure Software	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.	2026-08-05	4.8	CVE-2026-20198

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco IOS XE Software	A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, remote attacker with low privileges to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient error handling in the web-based management interface. An attacker could exploit this vulnerability by authenticating with a malformed certificate. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2026-08-05	6.3	CVE-2026-20311
Cisco--Cisco IOS XE Software	A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, remote attacker with low privileges to perform a denial of service (DoS) attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface of an affected device. A successful exploit could allow the attacker to cause the web-based management interface to become unresponsive.	2026-08-05	4.3	CVE-2026-20308
Cisco--Cisco RoomOS Software	A vulnerability in the logging subsystem of Cisco RoomOS could allow an authenticated, local attacker with low privileges to access sensitive information. This vulnerability is due to the logging of sensitive information. An attacker could exploit this vulnerability by enabling a specific logging level and then collecting the system logs. A successful exploit could allow the attacker to view sensitive information like user login credentials.	2026-08-05	5.7	CVE-2026-20289
Cisco--Cisco Terminal Services Agent	A vulnerability in the network driver of Cisco Terminal Service (TS) Agent could allow an authenticated, remote attacker to bypass firewall rules that are associated with the account of the attacker. This vulnerability is due to an incorrect mapping of network connections to user accounts. An attacker with at least user-level credentials could exploit this vulnerability by sending crafted network traffic to an affected device. A successful exploit could allow the attacker to inherit the firewall rules associated with a different user in the system.	2026-08-05	5	CVE-2026-20028
Cisco--Cisco Unified Computing System (Standalone)	A vulnerability in the web-based management interface of Cisco IMC could allow an authenticated, remote attacker with Admin privileges to execute arbitrary commands on the underlying operating system of an affected system and elevate privileges to root. This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by entering crafted inputs to the web-based management interface of the affected software. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system as the root user. Cisco has assigned this vulnerability a SIR of High rather than Medium as the score indicates because additional security implications could occur when the attacker becomes root.	2026-08-05	6.5	CVE-2026-20288
CloudFoundry Foundation--BOSH	Path Traversal in BOSH-Ecosystem / BOSH allows an IaaS-metadata attacker to make the agent write a root-owned file with partially attacker-controlled body to any path ending in .network, and create any missing parent directories with mode 0777 via network Alias on Ubuntu. Affected versions: BOSH agent < v2.847.0 (jammy <= v1.1202, or noble <= v1.364). Lower bound unspecified in advisory ("All bosh agent versions").	2026-08-06	4.2	CVE-2026-41861
code-projects--Task Management System	A vulnerability was found in code-projects Task Management System 1.0. This affects an unknown part of the file /user/UpdateTaskStatus.php. The manipulation of the argument task_id/val results in missing authorization. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2026-08-09	6.5	CVE-2026-19345
code-projects--Task Management System	A vulnerability was found in code-projects Task Management System 1.0. This issue affects some unknown processing of the file /user/CommentSave.php. The manipulation of the argument comment/task_id/minid/recId/myName/myImage results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2026-08-09	4.3	CVE-2026-19378

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codesupplyco--Powerkit	Contributor Cross Site Scripting (XSS) in Powerkit <= 3.1.0 versions.	2026-08-06	6.5	CVE-2026-28178
Colissimo--Colissimo Officiel : Mthodes de livraison pour WooCommerce	Customer Insecure Direct Object References (IDOR) in Colissimo Officiel : MÃfÃ©thodes de livraison pour WooCommerce <= 2.10.0 versions.	2026-08-06	4.3	CVE-2026-66692
cosmicstack-labs--mercury-agent	A vulnerability has been found in cosmicstack-labs mercury-agent up to 1.1.12. This vulnerability affects the function PermissionManager.checkShellCommand of the file src/capabilities/permissions.ts of the component run_command Handler. Such manipulation leads to incorrect privilege assignment. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	6.3	CVE-2026-18996
cosmicstack-labs--mercury-agent	A vulnerability was found in cosmicstack-labs mercury-agent up to 1.1.12. This issue affects the function Agent.handleBgCommand of the file src/core/agent.ts of the component bg Command Handler. Performing a manipulation results in incorrect authorization. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	6.3	CVE-2026-18997
cosmicstack-labs--mercury-agent	A vulnerability was determined in cosmicstack-labs mercury-agent up to 1.1.12. Impacted is the function SubAgent.run of the file src/core/sub-agent.ts of the component delegate_task Tool. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	6.3	CVE-2026-18998
Cozumslabs--Profile Builder	Unauthenticated Broken Access Control in Profile Builder <= 3.16.5 versions.	2026-08-06	5.3	CVE-2026-66701
cozumslabs--TranslatePress Translate Multilingual sites with AI Translation	The Translate Multilingual sites - TranslatePress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 's' parameter in versions up to, and including, 3.2.5. This is due to the translate_page() function unconditionally replacing the plugin's internal #!trpst# and #!trpen# marker tokens with literal angle brackets across the entire HTML page output after WordPress has already sanitized and escaped user input - allowing the attacker to bypass WordPress's normal HTML escaping by using these tokens, which are not HTML special characters, in the search query. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a specially crafted link.	2026-08-05	6.1	CVE-2026-17505
Damian Gra--FiboSearch	Shop manager Cross Site Scripting (XSS) in FiboSearch <= 1.33.0 versions.	2026-08-06	5.9	CVE-2026-28179
danpros--HTMLy	A vulnerability was identified in danpros HTMLy up to 3.1.1. Affected by this issue is the function unlink of the file /system/htmly.php of the component Delete Username Endpoint. Such manipulation of the argument File leads to path traversal. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	5.4	CVE-2026-18644
danpros--HTMLy	A security flaw has been discovered in danpros HTMLy up to 3.1.1. This affects the function add_content of the file /system/admin/admin.php of the component Admin Content Endpoint. Performing a manipulation of the argument oldfile results in path traversal. The attack may be initiated remotely. The exploit has been	2026-08-03	5.4	CVE-2026-18645

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.			
danpros--HTMLy	A weakness has been identified in danpros HTMLy up to 3.1.1. This vulnerability affects unknown code of the file /system/htmlly.php of the component Author Name Handler. Executing a manipulation of the argument Name can lead to path traversal. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	5.3	CVE-2026-18646
dartiss--code-embed	The Code Embed WordPress plugin prior to version 2.6.1 is vulnerable to stored Cross-Site Scripting (XSS) through the external URL embed feature in post content. The vulnerable code scans rendered content for URL embed tokens, fetches the remote URL, and inserts the remote response body into the page without output sanitization or an 'unfiltered_html' capability check. This allows a Contributor attacker to submit a pending post containing an inert-looking URL token that executes attacker-controlled JavaScript when an Administrator or Editor previews or reviews the post. This is distinct from CVE-2026-2512, which affected custom field meta values up to version 2.5.1. This vector affects version 2.6 and uses the documented external URL embed feature in post content. This particular issue is patched in version 2.6.1.	2026-08-07	6.5	CVE-2026-48093
DataPress (Dataverse Integration)--DataPress (Dataverse Integration)	The DataPress (Dataverse Integration) WordPress plugin before 2.91 does not properly restrict access to its template rendering feature and exposes the viewing user's data to it, allowing users with a role as low as Contributor to disclose sensitive information, such as the session cookies of higher privileged users who view the affected content.	2026-08-06	6.8	CVE-2026-5336
decidim--decidim	Decidim is a participatory democracy framework. Prior to 0.30.9, from 0.31.0 before 0.31.5, and in 0.32.0.rc1 before 0.32.0.rc2, the /admin/csv_census/census_logs record-management endpoints do not enforce full administrator authorization before rendering or mutating Decidim::Verifications::CsvDatum, allowing a participant manager to create, alter, or remove census records. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.	2026-08-06	6	CVE-2026-45415
decidim--decidim	Decidim is a participatory democracy framework. Prior to 0.30.9, from 0.31.0 before 0.31.5, and in 0.32.0.rc1 before 0.32.0.rc2, when VAPID delivery is enabled, the notification subscription flow stores a client-supplied push endpoint without validating that it belongs to an approved push service, and SendPushNotification later passes that endpoint to WebPush.payload_send, allowing an authenticated user to create stored, mostly blind server-side requests to arbitrary reachable HTTPS endpoints. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.	2026-08-06	6.4	CVE-2026-45573
decidim--decidim	Decidim is a participatory democracy framework. Prior to 0.30.9, from 0.31.0 before 0.31.5, and in 0.32.0.rc1 before 0.32.0.rc2, an administrator with landing-page editing privileges can store arbitrary HTML and JavaScript in an HTML content block, which Decidim::ContentBlocks::HtmlCell#html_content renders without sanitization, causing the script to execute in visitors' browsers. This issue is fixed in versions 0.30.9, 0.31.5, and 0.32.0.rc2.	2026-08-06	4.8	CVE-2026-45572
Deciso B.V.--OPNsense	OPNsense before 26.1.9 contains a stored cross-site scripting vulnerability that allows authenticated attackers with firewall rule management privileges to inject arbitrary HTML or JavaScript by embedding payloads in the firewall rule description field via the filter API endpoint. The unsanitized description value is persisted and later rendered through the default cell formatter in opnsense_bootgrid.js, which assigns raw cell content to innerHTML, causing injected scripts to execute in the browser of any authenticated user who views the Firewall Rules page, enabling session hijacking or credential theft.	2026-08-03	5.4	CVE-2026-49131

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Deciso B.V.--OPNsense	OPNsense before 26.1.9 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject arbitrary HTML or JavaScript by embedding payloads in the certificate description field via the trust certificate API. The unsanitized description value is persisted and later rendered in the Dashboard Certificates widget through Certificates.js, which interpolates the raw value into HTML attribute and text content sinks without encoding, causing injected scripts to execute in the browser of any authenticated user who views the Dashboard, enabling session hijacking or credential theft.	2026-08-03	5.4	CVE-2026-49132
DedeCMS--DedeCMS	A vulnerability has been found in DedeCMS up to 5.7.118 UTF8SP2. The affected element is the function _4_Setup of the file install/index.php of the component Installation Wizard. Such manipulation leads to file inclusion. The attack can be executed remotely. This attack is characterized by high complexity. The exploitability is described as difficult. The exploit has been disclosed to the public and may be used.	2026-08-09	5	CVE-2026-19353
Dell--Dell OpenManage Server Administrator Managed Node (Patch) for Windows	Dell OpenManage Server Administrator, versions prior to 11.1.0.2, contains a Relative Path Traversal vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Filesystem access for attacker.	2026-08-07	6.5	CVE-2026-56794
Dell--Monitor driver	Dell Monitor driver, version 1.0.0.0, contains an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-08-03	6.6	CVE-2026-40717
Dell--RVTools	Dell RVTools versions prior to 4.8.1, contains an improper certificate validation vulnerability in the collector. A remote unauthenticated attacker could potentially exploit this vulnerability leading to loss of confidentiality and integrity.	2026-08-06	6.8	CVE-2026-64993
dgtlmoon--changedetection.io	changedetection.io's /settings save handler builds an update dict from form.data['application'] and blind-merges it into the stored application settings via .update(). Because WTForms represents an unchecked checkbox as False rather than 'unchanged', and only the 'password' field is special-cased against this problem, a POST to /settings that omits the api_access_token_enabled field (e.g. a minimal scripted request) silently disables API key enforcement for the entire REST API, exposing the full watch list, history, and configuration to unauthenticated requests.	2026-08-05	6.3	CVE-2026-71204
dgtlmoon--changedetection.io	changedetection.io's /login route checks the submitted password against a single PBKDF2-HMAC-SHA256 hash with no per-IP or per-session rate limiting, failed-attempt counter, or lockout (no rate-limiting library is present in requirements.txt). Because the entire application is protected by one shared password with no per-user accounts, a successful brute-force guess grants full administrative access, including the ability to view/regenerate the API token.	2026-08-05	6.5	CVE-2026-71205
dgtlmoon--changedetection.io	changedetection.io's REST API resources are protected by an @auth.check_token decorator validating the caller's x-api-key header, except the Spec resource registered at /api/v1/full-spec (changedetectionio/api/Spec.py), whose get() method carries neither @auth.check_token nor @validate_openapi_request. An unauthenticated client can retrieve the full merged OpenAPI schema (all endpoint paths, parameters, and registered processor plugins) even when API access control is enabled and every sibling /api/v1/* route correctly requires the key.	2026-08-05	5.3	CVE-2026-71203
diaowen--DWSurvey	A vulnerability was found in diaowen DWSurvey up to 6.14.0. Impacted is the function in DwDeisgnSurveyController.devSurvey. of the file /api/dwsurvey/app/v6/dw-design-survey/dev-survey.do of the component Survey Handler. The manipulation results in authorization bypass. The attack can be	2026-08-04	6.3	CVE-2026-18722

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.			
diaowen--DWSurvey	A vulnerability was determined in diaowen DWSurvey up to 6.14.0. The affected element is an unknown function of the file /api/dwsurvey/app/survey/up-survey-status.do of the component Survey Status Handler. This manipulation causes improper authorization. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	6.3	CVE-2026-18723
diboot--diboot-core	diboot-core's POST /common/load-related-data endpoint resolves caller-supplied field names to any @TableField column of any entity and returns those values for all rows, with no field or entity allowlist. The only guard, relatedDataSecurityCheck(), returns true unconditionally, so any authenticated user (including a zero-role account) can read @JsonIgnore-annotated secret fields such as lamAccount.authSecret and lamAccount.secretSalt for every account, or arbitrary secret fields of any other entity. Shiro's two-iteration MD5 with an 8-character salt is trivially crackable offline, so the disclosed admin password hashes convert to full administrative takeover. The endpoint is not example code; the official diboot-admin-ui frontend requires it, so deployments following the vendor's recommended integration expose it. The mechanism was renamed relatedData* to attachMore* on the development branch, but attachMoreSecurityCheck() also returns true unconditionally.	2026-08-06	6.5	CVE-2026-70557
DjangoCRM--django-crm	DjangoCRM's toggle_default_sorting view is the only route in common/urls.py that is not wrapped in login_required or staff_member_required, and it redirects to a caller-supplied next_url GET parameter after only checking secure_url(next_url), which merely verifies the target host matches the current site's domain (blocking only cross-domain redirects) while allowing any same-site path with no authentication required to reach the view. This enables unauthenticated phishing redirects and referrer-based token leakage via redirect chains.	2026-08-05	4.3	CVE-2026-71240
django--Django	An issue was discovered in Django 5.2 before 5.2.17 and 6.0 before 6.0.8. `django.contrib.admin.utils.display_for_field()` renders `URLField` values as clickable links in the admin without validating the URL. A value stored with an unsafe scheme is displayed as a link on changelist and read-only admin pages, which allows cross-site scripting against staff users who click the link. Exploitation requires the unsafe value to already be stored in the database. `URLField` validation through a `ModelForm` or the admin rejects unsafe schemes, so this affects applications that persist `URLField` data without running model validation, for example through direct queryset writes, deserialization, or bulk import of untrusted input. Django would like to thank Egor Saltykov for reporting this issue.	2026-08-04	6.1	CVE-2026-15920
django--Django	An issue was discovered in Django 5.2 before 5.2.17 and 6.0 before 6.0.8. `django.utils.translation.check_for_language()` is subject to a potential denial-of-service attack when given many distinct, very long language codes, which are retained as keys in an in-memory cache and consume process memory. Such codes reach the function through the `django.views.i18n.set_language()` view, which is not routed by default. The consumed memory is bounded, since request data is limited by the `DATA_UPLOAD_MAX_MEMORY_SIZE` setting (default 2.5 MB) and the cache holds a fixed maximum number of entries. Earlier, unsupported Django series (such as 5.1.x, 5.0.x, and 4.2.x) were not evaluated and may also be affected. Django would like to thank Jaeyoung Jang for reporting this issue.	2026-08-04	5.3	CVE-2026-15337
django--Django	An issue was discovered in Django 5.2 before 5.2.17 and 6.0 before 6.0.8. GeoDjango's `django.contrib.gis.geos.GEOSGeometry` is subject to a potential denial-of-service when parsing deeply nested `GEOMETRYCOLLECTION` objects supplied as well-known text (WKT), well-known binary (WKB), or hex-encoded WKB, which triggers unbounded recursion and a segmentation fault in the underlying GEOS library. Spatial field lookups and the `django.contrib.gis.forms.GeometryField` form field are also affected. Earlier,	2026-08-04	5.3	CVE-2026-15830

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unsupported Django series (such as 5.1.x, 5.0.x, and 4.2.x) were not evaluated and may also be affected. Django would like to thank Andrew MacPherson and kimchunbok_ for reporting this issue.			
dmitriiweb--article-scraper-mcp	A vulnerability was detected in dmitriiweb article-scraper-mcp 1.0.0. This vulnerability affects the function fetch_article of the file news_scraper_mcp/server.py. The manipulation of the argument url results in server-side request forgery. The attack may be performed from remote. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	6.3	CVE-2026-19375
documenso--documenso	Documenso's sign-field-with-token.ts, used by the live document-signing UI, allows a recipient with the ASSISTANT role to fetch and complete fields belonging to any later-or-equal-order, not-yet-signed recipient in the same envelope, with no restriction on field type. The handler upserts a Signature record tied to the target field's recipientId with no check that field.type is SIGNATURE and the acting recipient owns it. A newer V2 signing path (sign-envelope-field.ts) explicitly blocks assistants from completing SIGNATURE fields, and the project's own test suite comments confirm this guard is absent from the V1 path used here. In a sequential-signing document, an assistant recipient can therefore forge another signer's signature field.	2026-08-05	6.5	CVE-2026-71247
Dokan, Inc.--Dokan	Custom role Broken Access Control in Dokan <= 5.0.10 versions.	2026-08-06	5.3	CVE-2026-66699
Dolibarr--ERP	A vulnerability has been found in Dolibarr ERP up to 23.0.3. Affected is the function fail of the file htdocs/takepos/invoice.php of the component TakePOS Module. Such manipulation leads to missing authorization. The attack may be performed from remote. The name of the patch is 8992ce8704da947b6abe7b65a6fe59aed736bb81. It is advisable to implement a patch to correct this issue.	2026-08-09	6.3	CVE-2026-19350
Domoticz--Domoticz	Domoticz versions prior to 2026.3 contains a stored cross-site scripting vulnerability in the mobile dashboard that allows authenticated attackers to inject arbitrary HTML and JavaScript by updating Text or Alert subtype device values through the API. The mobile dashboard renders device data via ng-bind-html with only an nl2br() transform that performs no HTML escaping, allowing attackers to store malicious payloads that execute in any administrator's browser upon viewing the mobile dashboard, enabling session cookie theft and account takeover.	2026-08-07	4.4	CVE-2026-11425
duckdb--duckdb-aws	The DuckDB AWS extension for DuckDB contains a security policy bypass vulnerability that allows any database user with SQL execution permissions to extract plaintext AWS credentials by calling the load_aws_credentials function with the redact_secret parameter set to false, circumventing the database-wide allow_unredacted_secrets=false policy. Attackers can invoke this single function to retrieve the underlying AWS credential chain including access_key_id, secret_access_key, session_token, and region in plaintext, which are immediately valid against AWS APIs and particularly impactful in managed environments where pg_duckdb is preloaded and an AWS credential chain such as IMDSv2, IRSA, ECS task role, or EC2 instance role is reachable.	2026-08-03	6.5	CVE-2026-58139
Easy Booking--Easy Booking	The Easy Booking WordPress plugin before 3.5.0 does not re-enforce a bookable product's configured minimum booking duration on the server side when adding to cart and calculating the booking price, allowing unauthenticated users to place below-minimum bookings and complete underpriced orders.	2026-08-06	5.3	CVE-2026-14831
Ehco1996--django-sspanel	A weakness has been identified in Ehco1996 django-sspanel up to 2023.12.26. This affects the function TicketDetailView of the file apps/sspanel/views.py of the component Support Ticket Handler. Executing a manipulation can lead to authorization bypass. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	2026-08-04	6.3	CVE-2026-18818

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ELAN Microelectronics Corp.--ELAN Smart-Pad	A stack-based buffer overflow vulnerability exists in ELAN Microelectronics Corp. ELAN Smart-Pad on Windows (ETD.sys and ETDSMBus.sys). During Intel SMBus recovery, ETDSMBus.sys does not enforce an upper-bound check on the hardware-derived report count, allowing an out-of-range value to be forwarded to ETD.sys where it is used as a loop counter for a stack buffer copy without destination size validation. A local attacker with standard user privileges can trigger a kernel bugcheck (BSOD 0xF7 DRIVER_OVERRAN_STACK_BUFFER), resulting in denial of service. This issue affects ELAN Smart-Pad through ETD24.21.52.3.	2026-08-06	4.7	CVE-2026-18909
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3, the check Electron uses on macOS to confirm it was launched by a same-signed parent process could be bypassed by a local process. Apps that enable fuse-based hardening restricting ELECTRON_RUN_AS_NODE and NODE_OPTIONS to same-signed parents rely on this check, and a local attacker could bypass it and run code inside the signed app, inheriting its TCC permissions and keychain access. This issue is fixed in 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3.	2026-08-05	6.3	CVE-2026-70597
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3, extension tab and scripting APIs were not scoped to the extension's own session. A malicious or compromised extension loaded into one session could navigate, script, and read from windows belonging to a different session. Apps are only affected if they load Chrome extensions via session.loadExtension and rely on separate sessions to isolate that extension from other content. This issue is fixed in versions 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3.	2026-08-05	6.6	CVE-2026-70602
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.6, 40.9.0, 41.1.1, and 42.0.0-beta.1, shell.openPath() did not reject paths containing embedded null bytes. Apps that perform string-only validation of file paths, for example checking the file extension, before passing them to shell.openPath() could be bypassed, allowing an attacker-controlled path to open a different file than the one that passed validation. Apps are only affected if they pass paths derived from untrusted input to shell.openPath() and rely on string-based validation without a filesystem check. This issue is fixed in versions 39.8.6, 40.9.0, 41.1.1, and 42.0.0-beta.1.	2026-08-05	6	CVE-2026-70603
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.9, 40.9.2, 41.2.1, and 42.0.0-beta.3, the DevTools reveal in file manager action could launch the target file rather than reveal it. An attacker with a separate means of running script inside the DevTools frontend, such as a malicious DevTools extension, could use showItemInFolder handling to execute native code outside the sandbox when DevTools is opened for windows exposed to untrusted content or untrusted DevTools extensions. This issue is fixed in 39.8.9, 40.9.2, 41.2.1, and 42.0.0-beta.3.	2026-08-05	6.9	CVE-2026-70611
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.7, 40.9.0, 41.2.0, and 42.0.0-beta.1, serial-port and media permission checks made from an iframe passed the top-level frame origin to session.setPermissionCheckHandler instead of the requesting iframe origin. Origin-based handler logic could grant a cross-origin iframe device access intended only for the top-level origin. This issue is fixed in 39.8.7, 40.9.0, 41.2.0, and 42.0.0-beta.1.	2026-08-05	5.9	CVE-2026-70599
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3, when following HTTP redirects, net.fetch() and net.request() did not restrict which schemes a redirect could target. A remote server could redirect a request to a local resource, and if the app returns or forwards the response body, local file contents could be disclosed. Apps are only affected if they make net requests to attacker-	2026-08-05	5.9	CVE-2026-70605

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	influenced URLs with redirects followed and expose the response body. This issue is fixed in versions 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3.			
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 40.10.6, 41.9.1, 42.5.1, and 43.0.0, when a custom protocol handler returned a ProtocolResponse with a url and no session, Electron made the upstream request through defaultSession instead of the session that handled the protocol. A cached response could then be reused across otherwise isolated session partitions. Apps that use ProtocolResponse.url, omit ProtocolResponse.session, and rely on separate sessions to isolate content are affected. This issue is fixed in versions 40.10.6, 41.9.1, 42.5.1, and 43.0.0.	2026-08-05	5.9	CVE-2026-70606
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3, some window options supplied by web content in the window.open() features string were applied to the new BrowserWindow without an allowlist. Untrusted content could set window options it should not control, including options that cause the main process to access attacker-chosen file or network paths, when untrusted content can call window.open() and the app does not override child window options via setWindowOpenHandler or overrideBrowserWindowOptions. This issue is fixed in 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3.	2026-08-05	5.3	CVE-2026-70607
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.7, 40.9.0, 41.2.0, and 42.0.0-beta.1, the mode option of webContents.openDevTools() was not sanitized before use by the DevTools frontend. If an attacker can influence this value, script under their control may run in the DevTools context, which in unsandboxed configurations has access to Node.js, including when untrusted input reaches the mode argument of openDevTools() or untrusted content calls openDevTools() on a webview it embeds. This issue is fixed in 39.8.7, 40.9.0, 41.2.0, and 42.0.0-beta.1.	2026-08-05	5.7	CVE-2026-70609
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.9, 40.9.2, 41.2.2, and 42.0.0-beta.4, objects copied across the contextBridge boundary from untrusted content could carry an attacker-influenced prototype, enabling prototype-pollution-style attacks against preload code despite context isolation being enabled. Apps are only affected if their preload code accepts object arguments from untrusted content and reads properties from them without own-property checks, while apps that only accept primitive arguments or validate object arguments are not affected. This issue is fixed in 39.8.9, 40.9.2, 41.2.2, and 42.0.0-beta.4.	2026-08-05	5.4	CVE-2026-70610
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3, requests to open external protocol URLs from web content did not take iframe sandbox restrictions into account, so a sandboxed iframe could cause an OS-registered external application to be launched. The frame sandbox state was also not made available to the app permission handlers, affecting apps that render untrusted content in sandboxed iframes and grant the openExternal permission by default when no setPermissionRequestHandler is installed. This issue is fixed in 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3.	2026-08-05	5.4	CVE-2026-70612
Endress+Hauser--FDI Package library	A vulnerability in the iDTM FDI allows an attacker with elevated privileges and access to the host system to enable the debug interface by placing a crafted file in the application directory, potentially resulting in unauthorized access to connected devices and exposure, modification, or disruption of device data or operation.	2026-08-03	6.7	CVE-2026-9593
esphome--esphome	ESPHome through 2026.7.0-dev discloses plaintext passwords via its web_server component. In WebServer::text_json_() (esphome/components/web_server/web_server.cpp), a text entity configured with mode: password (TEXT_MODE_PASSWORD) has its JSON "state" field correctly masked as "*****", but the same serialization path unconditionally writes the	2026-08-05	6.5	CVE-2026-71260

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	raw password into the JSON "value" field via set_json_icon_state_value()/set_json_value(). Because web_server listens on port 80 with no authentication by default, any attacker on the local network can retrieve the plaintext password (e.g. WiFi credentials, API tokens) via GET /text/<entity_id> or the /events EventSource stream.			
Eugeniy--russh	Russh is a Rust SSH client & server library. Prior to 0.62.5, russh dispatches channel-scoped Handler callbacks for recipient channel IDs that were never opened or confirmed in russh/src/server/encrypted.rs, server_read_authenticated, and the exec_request callback. Version 0.62.5 fixes the issue.	2026-08-03	6.5	CVE-2026-68930
Eukaryot--sonic3air	Sonic 3 A.I.R. before commit 2492d18 contains a missing source address validation vulnerability in ConnectionManager where established connections are resolved by a two-byte local connection handle alone without verifying that the datagram source address matches the registered remote address for the connection. An on-path attacker who can observe cleartext UDP traffic can inject arbitrary packets into any established session by forging the two-byte connection identifier, enabling session termination via TerminateConnectionPacket, arbitrary channel message forgery, and forged request responses without requiring IP address spoofing.	2026-08-06	5.9	CVE-2026-66732
Event Booking Manager for WooCommerce (Pro)--Event Booking Manager for WooCommerce (Pro)	The Event Booking Manager for WooCommerce (Pro) WordPress plugin before 5.0.3 does not validate the ticket price on the server during its native (non-WooCommerce) checkout, trusting the per-ticket price supplied by the client instead of re-deriving the event's configured price. This allows unauthenticated users to book paid event tickets for free, obtaining completed bookings and valid tickets at no cost.	2026-08-06	5.3	CVE-2026-16067
Events Made Easy--Events Made Easy	The Events Made Easy WordPress plugin before 3.1.2 does not bind the payment authorization token to the payment record being charged, allowing unauthenticated attackers to pay a low amount for a cheap booking and have a separate, higher-priced booking marked as fully paid.	2026-08-06	5.3	CVE-2026-14842
facelessuser--pymdown-extensions	PyMdown Extensions is a set of extensions for the Python-Markdown markdown project. In versions up to and including 10.21.3, the b64 extension is vulnerable to a path traversal that discloses arbitrary files: it inlines images referenced by by joining the src onto the configured base_path with os.path.normpath and opening the result directly, without verifying that the resolved path stays inside base_path. As a result, an src containing ../ sequences or an absolute path reads a file outside base_path as long as it has an allowed image extension (.png, .jpg, .jpeg, .gif, .svg), and the file's contents are then base64-encoded into the rendered output, disclosing them. An application that renders untrusted Markdown with pymdownx.b64 enabled can therefore leak the contents of image-extension files readable by the process to whoever controls the Markdown or views the output, a targeted file-read bounded by the extension check. This issue has been fixed in version 11.0.	2026-08-06	5.3	CVE-2026-61632
FFmpeg--FFmpeg	FFmpeg versions from 3.0 up to, but not including, 9.0 contain an uninitialized heap memory read vulnerability in the native RSCC decoder (libavcodec/rsc.c) that allows attackers to disclose heap memory contents by supplying a crafted video file with a compressed tile that decompresses fewer bytes than the declared tile geometry requires. When rsc_decode_frame() calls av_image_copy_plane() without validating the decompressed byte count against the tile dimensions, the unwritten suffix of the persistent intermediate buffer ctx->inflated_buf is copied into the decoded frame, potentially exposing data from prior heap allocations or previous decoded frames in persistent decoding services.	2026-08-06	5.5	CVE-2026-70629
FFmpeg--FFmpeg	FFmpeg versions from 3.0 up to, but not including, 9.0 contain an uninitialized heap memory read vulnerability in the native Screenpresso decoder (libavcodec/screenpresso.c) that allows attackers to recover sensitive memory contents by supplying a crafted SPV1 packet with a valid zlib stream that	2026-08-06	5.5	CVE-2026-70630

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	decompresses fewer bytes than the full frame requires. The screenpresso_decode_frame() function fails to validate the produced byte count before calling av_image_copy_plane() to copy the complete frame dimensions from the persistent ctx->inflated_buf buffer, causing unwritten heap memory from prior allocations or prior frames to be copied into decoded output and potentially exposing sensitive data such as userspace addresses from persistent decoding services.			
FFmpeg--FFmpeg	FFmpeg versions from 0.5 up to, but not including, 9.0 contain an uninitialized heap memory disclosure vulnerability in the native TIFF decoder in libavcodec/tiff.c. An attacker who can cause FFmpeg to decode a crafted TIFF file can supply a valid Deflate-compressed strip that terminates successfully after producing fewer bytes than the declared strip requires. The tiff_unpack_zlib() function allocates a heap buffer sized for the full declared strip but copies all declared rows via memcpy() regardless of how many bytes zlib actually decompressed, causing unwritten bytes that can contain stale data from prior heap allocations to be incorporated into decoded image output and potentially exposing sensitive data in persistent services.	2026-08-06	5.5	CVE-2026-70631
firefly-iii--firefly-iii	Firefly III's webhook URL validator (IsValidWebhookUrl.php) filters most private/reserved IPv4 ranges but contains an explicit early-return that allows any resolved address in 127.0.0.0/8, permitting an authenticated user (with webhooks enabled, which is off by default) to configure a webhook targeting loopback services on the server. Additionally, the validator resolves the target hostname once via gethostbyname() at validation time, but the actual outbound request (StandardWebhookSender.php, via Guzzle) re-resolves the hostname independently at send time, allowing a DNS-rebinding attacker to pass validation against a public IP and have the real request delivered to a private or internal address. The webhook response body is only written to a server-side debug log, not returned to the triggering user, so this is a blind SSRF primitive rather than one with direct response read-back.	2026-08-05	4.3	CVE-2026-71250
Five Star Restaurant Reservations--Five Star Restaurant Reservations	The Five Star Restaurant Reservations WordPress plugin before 2.7.23 does not verify the authenticity of incoming payment notifications, failing to validate the payment recipient, amount, and status or to bind the notification to the intended booking, allowing unauthenticated attackers to mark arbitrary pending reservations as paid and confirmed.	2026-08-06	5.3	CVE-2026-15147
Flarum--Flarum Framework	Flarum before 1.8.16 contains an improper session invalidation vulnerability that allows attackers who hold a valid session token to retain full account access after a victim changes their password, because the access_tokens table is never cleared on password change events. The TokensClearer::clearPasswordTokens() function only removes rows from the password_tokens table while leaving all active session cookies and API bearer tokens intact, including long-lived RememberAccessToken entries, and administrator-forced password resets via the user update endpoint are equally ineffective at revoking attacker-held sessions.	2026-08-05	6.8	CVE-2026-39924
fledge-iot--fledge	Fledge's backup-restore upload handler, upload_backup() (python/fledge/services/core/api/backup_restore.py), calls tarfile.extractall(temp_path) on an admin-uploaded tar archive with no filter argument and no per-member path validation. A crafted tar archive containing member names with `./` path components extracts files outside the intended temporary directory, allowing arbitrary file writes anywhere on the filesystem reachable by the Fledge process. Requires the admin role (@has_permission("admin")).	2026-08-05	4.9	CVE-2026-71283
Formidable Forms--Formidable Forms	The Formidable Forms WordPress plugin before 6.32.1 does not properly validate the status of a PayPal subscription payment before marking it complete, allowing unauthenticated users to bypass payment and trigger paid form actions - such as	2026-08-06	5.9	CVE-2026-11361

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	digital content access, license delivery, and membership activation - without being charged.			
FoundationAgents--MetaGPT	A vulnerability was found in FoundationAgents MetaGPT up to 0.8.2. The impacted element is the function DataInterpreter of the file metagpt/roles/di/data_interpreter.py. The manipulation results in code injection. The attack must be initiated from a local position. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	5.3	CVE-2026-19058
FoundationAgents--MetaGPT	A vulnerability was identified in FoundationAgents MetaGPT up to 0.8.2. This impacts an unknown function. Such manipulation leads to code injection. The attack needs to be performed locally. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	5.3	CVE-2026-19060
getgrav--grav-plugin-form	The Grav form plugin (getgrav/grav-plugin-form) before 9.1.13 contains an open redirect vulnerability. Since v9.1.11, the redirect process action evaluates user-supplied form data inside Twig expressions, and Grav::redirect() accepts external URLs without origin validation. When a form blueprint defines a redirect target such as redirect: "{ form.value('next') }" using an attacker-controllable field, an unauthenticated form submitter can supply a value like https://evil.com to cause a 302 redirect to an arbitrary external site, enabling phishing.	2026-08-03	6.5	CVE-2026-69087
GetPaid--GetPaid	The GetPaid WordPress plugin before 2.8.55 does not verify the authenticity of incoming Worldpay payment notifications, allowing unauthenticated attackers to forge a notification that marks a pending invoice as paid without any payment being made.	2026-08-06	5.9	CVE-2026-12901
ggml-org--llama.cpp	llama.cpp builds b5702 through b7653 contain an out-of-bounds read vulnerability in the recurrent memory state restore path that allows attackers with write access to the slot save directory to read memory past the end of the allocated cells array. Attackers can craft a malicious slot file with an oversized seq_id value to trigger an out-of-bounds read that leaks heap data including pointer values into server logs, defeating ASLR protections and facilitating further exploitation.	2026-08-06	6.5	CVE-2026-43630
ggml-org--llama.cpp	llama.cpp builds b1886 through b7445 contain a null pointer dereference vulnerability in the LLaMA-Android JNI wrapper where the bench_1model() function fails to validate the model context pointer before dereferencing it. Attackers can supply a malicious, corrupt, or truncated model file to trigger a null context condition, causing a SIGSEGV crash that terminates the Android application process and results in denial of service.	2026-08-06	5.5	CVE-2026-70639
ghostfolio--ghostfolio	Ghostfolio is an open source wealth management software. Prior to version 3.4.0, Ghostfolio's Stripe checkout success-URL handler at `GET /api/v1/subscription/stripe/callback?checkoutSessionId=<id>` retrieves the Stripe Checkout Session by ID and unconditionally grants a Premium subscription to the session's `client_reference_id` - without ever checking `session.payment_status` or `session.status`. There is no separate Stripe webhook endpoint with `stripe-signature` verification; this callback is the sole code path that creates Stripe-driven subscriptions. Any authenticated user can self-grant a 1-year Premium subscription without ever paying. Version 3.4.0 rejects sessions unless `session.payment_status` === `paid` AND `session.status` === `complete` (fails closed). Additionally, new unique `stripeCheckoutSessionId` column a session can't be redeemed twice (race-safe via DB unique constraint).	2026-08-07	6.5	CVE-2026-47127
GitroomHQ--postiz-app	An issue in the billing and license activation subsystem allows remote attackers to bypass payment authorization workflows. By exploiting insufficient cryptographic validation or lack of server-side state verification on promotional/lifetime-deal (LTD) redemption codes, an unauthenticated attacker can forge valid redemption	2026-08-06	6.5	CVE-2026-19127

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	tokens or replay existing single-use codes to activate permanent, tier-highest paid subscriptions without a financial transaction.			
GL.iNet--E5800	A security vulnerability has been detected in GL.iNet E5800, E750, X2000, X3000, XE3000 and XE300 up to 20260707. Impacted is an unknown function of the file /sdk/v1 of the component eSIM LPA API. Such manipulation leads to improper authorization. The attack can only be initiated within the local network. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	5.4	CVE-2026-18584
GL.iNet--MT3000	A vulnerability was detected in GL.iNet MT3000, MT6000, BE9300, BE3600, MT3600BE, E5800, BE6500, MT5000, X3000, XE3000 and MT2500 up to 20260707. The affected element is the function nas-web.get_file_list of the component APPS-NAS Module. Performing a manipulation results in heap-based buffer overflow. The attack may be initiated remotely. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.	2026-08-03	4.3	CVE-2026-18585
gm_alex--User Access Manager	The User Access Manager plugin for WordPress is vulnerable to Second-Order SQL Injection via the 'id' parameter of the wp_ajax_save-attachment-compat AJAX action in versions up to, and including, 2.3.12. This is due to insufficient validation on the objectId value stored in the saveAjaxAttachmentData() function and subsequent unparameterized concatenation in the addQueryExcludedPostFilter() function - the stored value is later retrieved from the database and used as an array key, then directly imploded into a SQL NOT IN() clause without integer casting or prepared statements. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-05	6.5	CVE-2026-15281
GNOME--Epiphany	A flaw was found in Epiphany. An issue in how the browser reads web addresses allows attackers to fake the domain name shown in the address bar. If a user clicks a specially crafted link containing a colon (for example, https://trusted.com:80@attacker.com/), the address bar and security menus will display the safe website (trusted.com) but it will actually load the attacker website (attacker.com) on the screen. This allows attackers to create convincing phishing pages to trick users into trusting a malicious site.	2026-08-06	5.4	CVE-2026-18487
go-git--go-git	go-git is an extensible git implementation library written in pure Go. Prior to 5.19.2 and 6.0.0-alpha.5, reference names are not sanitized before being used to construct on-disk paths under the reference storage directory, so a maliciously crafted reference name (for example containing directory-traversal sequences) can cause go-git to write files outside the intended reference storage directory. Versions 5.19.2 and 6.0.0-alpha.5 fix the issue.	2026-08-07	6.3	CVE-2026-71557
guzzle--guzzle	Guzzle is an extensible PHP HTTP client. Prior to 7.15.2 and 8.0.1, SetCookie::matchesDomain() gives every subdomain of a cookie Domain that cookie unless SetCookie::matchesDomain() recognizes the Domain as an IP literal or a numeric host, and the decision comes from the domain's own text, so two spellings a transport reads as an address keep subdomain scope. Hexadecimal and mixed-base forms such as 0x7f000001 and 0177.0.0.0x1 go unrecognized while libcurl 8.21.0 reads both as 127.0.0.1. A percent-escaped Domain keeps that scope on both branches because percent-decoding sits above numeric parsing, so 192.168.0.%31 and 127.0.0.1%2e are registered names in the URI grammar rather than address literals, and no numeric rule in any base classifies them, while libcurl decodes the host before resolving and reads them as 192.168.0.1 and 127.0.0.1. A cookie stored for Domain=0x7f000001 is placed in the Cookie header of a request to evil.0x7f000001, disclosing a session identifier or token to a host that is not that address, and a response from evil.0x7f000001 setting Domain=0x7f000001 is accepted into the jar and replayed to the address, so a server answering for the look-alike name can fix a session or set application state. Exploitation requires the	2026-08-03	6.5	CVE-2026-69245

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application to enable cookie support, address an origin by one of these spellings, and contact a host whose name ends in that spelling. This issue is fixed in versions 7.15.2 and 8.0.1.			
Handwriting-OCR--handwriting-ocr-mcp-server	A security flaw has been discovered in Handwriting-OCR handwriting-ocr-mcp-server 0.1.0. Affected by this vulnerability is the function fs.readFileSync of the file src/index.ts of the component upload_document. Performing a manipulation of the argument File results in path traversal. Attacking locally is a requirement. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19372
hapifhir--org.hl7.fhir.core	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to 6.9.11, the hidden scan command concatenates attacker-controlled Implementation Guide titles, profile titles, and source references into scan.html without escaping in Scanner.java. As a result, a user who scans an attacker-supplied IG/profile and then opens or publishes the generated local/CI HTML report can trigger stored cross-site scripting, executing attacker-controlled JavaScript in the report's browser context. This issue is fixed in version 6.9.11.	2026-08-07	5	CVE-2026-62293
HashiCorp--Consul	Consul Community Edition and Consul Enterprise 1.18.21 through 2.0.2 are vulnerable to a partial arbitrary file read when configured to use the Vault Connect CA provider with JWT or AppRole authentication. A privileged attacker with 'operator:write' permission may direct Consul to read and forward credential files outside the intended scope, potentially leading to the exfiltration of sensitive secrets from the Consul server host. This vulnerability, CVE-2026-19017, is fixed in Consul 2.0.3 and Consul Enterprise 1.21.17, 1.22.11, and 2.0.3.	2026-08-07	6.8	CVE-2026-19017
HashiCorp--Consul	Consul Community Edition and Consul Enterprise 1.18.0 through 2.0.2 are vulnerable to an authenticated denial of service in the Enterprise-to-Community Edition downgrade path that may allow an authorized caller to crash the Consul server. A caller with config-entry write permission can submit a service-router configuration entry that causes the agent to exit unexpectedly. This vulnerability, CVE-2026-19012, is fixed in Consul 2.0.3 and Consul Enterprise 1.21.17, 1.22.11, and 2.0.3.	2026-08-07	5.3	CVE-2026-19012
HashiCorp--Consul	Consul Community Edition and Consul Enterprise 1.2.0 through 2.0.2 are vulnerable to an uncontrolled resource consumption issue in the Connect CA roots endpoint that may allow a remote caller to grow the agent's Connect CA roots cache without bound, defeating the operator's cache-disable configuration. This vulnerability, CVE-2026-19015, is fixed in Consul 2.0.3 and Consul Enterprise 1.21.17, 1.22.11, and 2.0.3.	2026-08-07	5.3	CVE-2026-19015
HashiCorp--Consul	Consul Community Edition and Consul Enterprise 1.3.0 through 2.0.2 are vulnerable to an unauthenticated denial of service in several agent HTTP API endpoints. A remote caller could cause the agent to consume substantial memory before the request was rejected. This vulnerability, CVE-2026-19113, is fixed in Consul 2.0.3 and Consul Enterprise 1.21.17, 1.22.11, and 2.0.3.	2026-08-07	5.3	CVE-2026-19113
HashiCorp--Consul	Consul Community Edition and Consul Enterprise 1.20.1 through 2.0.2 are vulnerable to an L7 intention authorization bypass when a service proxy is configured with a custom public listener. An authenticated mesh workload may reach HTTP paths that are blocked by a path-based deny intention. This vulnerability, CVE-2026-15970, is fixed in Consul 2.0.3 and Consul Enterprise 1.21.17, 1.22.11, and 2.0.3.	2026-08-07	4.2	CVE-2026-15970
HashiCorp--Consul	Consul Community Edition and Consul Enterprise 1.17.0 through 2.0.2 are vulnerable to an uncontrolled resource consumption issue in the Connect authorization endpoint that may allow a caller to grow the agent's intention-match cache without bound, defeating the operator's cache-disable configuration. This	2026-08-07	4.3	CVE-2026-19014

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability, CVE-2026-190124, is fixed in Consul 2.0.3 and Consul Enterprise 1.21.17, 1.22.11, and 2.0.3.			
HashiCorp--Consul	Consul Community Edition and Consul Enterprise 1.19.1 through 2.0.2 did not enforce the {{session:write}} ACL permission for session deletion operations submitted through the transaction API. An authenticated caller with network access to the Consul server RPC port could delete arbitrary sessions without holding the required permission. This vulnerability, CVE-2026-19016, is fixed in Consul 2.0.3 and Consul Enterprise 1.21.17, 1.22.11, and 2.0.3.	2026-08-07	4.2	CVE-2026-19016
HCL Software--HCL iControl	HCL iControl is affected by Weak SSL/TLS Version Supported vulnerability. It was observed that the application was using weak TLS versions such as TLS 1.0 and 1.1. These outdated protocols lack modern security features, making them vulnerable to known attacks and exposing sensitive information during data transmission.	2026-08-03	4.8	CVE-2026-56609
HCLSoftware--HCL Digital Experience and Digital Experience Compose	The default login portlet in HCL Digital Experience and Digital Experience Compose insufficiently protects credentials. Under certain very specific use cases and specific configurations, sensitive information may be written to web server logs. This only affects applications using the default login portlet.	2026-08-05	5.4	CVE-2026-21766
heshengtao--super-agent-party	A vulnerability was found in heshengtao super-agent-party up to 0.4.1. This affects the function get_file_content of the file server.py of the component execute_tool_manually Endpoint. The manipulation of the argument tool_name/tool_params results in information disclosure. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	5.3	CVE-2026-18974
Hewlett Packard Enterprise (HPE)--HPE Integrated Lights-Out 6 (iLO 6)	A potential denial of service vulnerability exists in HPE Integrated Lights-Out 6 (iLO 6) prior to v1.78.	2026-08-05	6.5	CVE-2026-63457
hfiref0x--LightFTP	LightFTP through 2.4 contains multiple data race vulnerabilities in ftpserv.c that allow anonymous attackers to cause undefined behavior by issuing LIST followed by ABOR commands without authentication. The control thread closes data_socket and file_fd descriptors while worker threads concurrently operate on the same fields in worker_thread_cleanup, allowing stale file descriptors to be reassigned by the OS and subsequently used by worker threads on unrelated resources, resulting in potential denial of service.	2026-08-06	5.9	CVE-2026-70637
HKUDS--nanobot	A security vulnerability has been detected in HKUDS nanobot up to 0.2.1. Impacted is the function ExecTool._guard_command/ExecTool._spawn of the file nanobot/agent/tools/shell.py of the component Shell Allowlist Handler. Such manipulation leads to os command injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 0.3.0 is recommended to address this issue. The name of the patch is 4562. It is advisable to upgrade the affected component. Multiple issues were reported to the project. They reacted with a high level of professionalism and kindness: "These five reports are variants of the same root cause: validation of shell commands containing multiple segments, wrappers, comments, or chained commands. The issue was fixed by validating every executable shell segment against the configured allowlist".	2026-08-07	6.3	CVE-2026-19243
HKUDS--nanobot	A vulnerability has been found in HKUDS nanobot up to 0.2.1. This affects the function _download_image_data_url of the file nanobot/providers/image_generation.py of the component Provider-returned Image URL Handler. The manipulation leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is 5095. It is recommended to apply a patch to fix this issue. The vendor explains: "We confirm that provider-	2026-08-07	6.3	CVE-2026-19246

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	returned image URLs required the same SSRF protections applied to other network retrieval paths. (...) The patch is currently available on main and is planned for the next patch release, v0.3.1."			
HKUDS--nanobot	A vulnerability was detected in HKUDS nanobot up to 0.2.1. The affected element is the function connect_mcp_servers of the file nanobot/agent/tools/mcp.py of the component MCP enabledTools Scope Handler. Performing a manipulation results in improper access controls. The attack is possible to be carried out remotely. The exploit is now public and may be used. Upgrading to version 0.3.0 is sufficient to fix this issue. The patch is named 4436. You should upgrade the affected component. Multiple issues were reported to the project. They reacted with a high level of professionalism and kindness: "Both reports describe the same root cause: MCP resource and prompt wrappers could be registered outside the intended enabledTools scope. The registration boundary was corrected".	2026-08-07	4.7	CVE-2026-19244
home-assistant--core	Home Assistant is open source home automation software focused on local control and privacy. Prior to 2026.6.1, the Android Companion app is vulnerable to an open redirect. The app passes the URL fragment from a homeassistant://invite deep link into the onboarding flow without ever displaying the destination hostname. Because no screen in the invitation or onboarding flow shows the parsed server URL before onboarding commits to it, a victim has no way to distinguish a legitimate invite from a malicious one. An attacker can craft an invite so that a single tap on the legitimate-looking "Connect to my Home Assistant server" button opens their /auth/authorize endpoint in the URL-less onboarding WebView, presenting a look-alike login page that captures the victim's credentials. Since invitations are intended to onboard brand-new users, targets are especially unlikely to notice the substitution. This issue is fixed in version 2026.6.1.	2026-08-07	4.3	CVE-2026-59717
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.34, the built-in CORS middleware, hono/cors, is vulnerable to a regular expression denial of service (ReDoS). During a preflight OPTIONS request, the middleware parses the attacker-controlled Access-Control-Request-Headers header using a whitespace-tolerant regular expression whose backtracking makes its running time quadratic in the input length. Because the header value is bounded only by the deployment's maximum HTTP header size, a single preflight carrying a long run of whitespace can consume seconds of CPU and block request processing. On runtimes that share one execution thread across requests, this stalls concurrent requests as well, and repeated requests can render the service unresponsive. This affects the default configuration, since the vulnerable path is reached whenever cors() is used with an unset or empty allowHeaders. Applications that set a non-empty allowHeaders are not affected. This issue is fixed in version 4.12.34.	2026-08-07	5.3	CVE-2026-69207
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. From 4.12.0 to 4.12.33, the languageDetector middleware is vulnerable to algorithmic complexity denial of service when processing a crafted language tag containing a large number of hyphen separated subtags. To implement progressive language tag truncation, normalizeLanguage() repeatedly calls parts.slice(0, i).join('-') for every possible prefix, so the total amount of string processing grows quadratically with the number of subtags. Language values may come from a query parameter, cookie, Accept-Language header, or URL path, depending on the detector configuration, and the default detector order enables query string, cookie, and header detection, so applications using languageDetector() may expose this processing to unauthenticated requests. An attacker may repeatedly send requests containing long, hyphen separated language tags, causing excessive CPU consumption and preventing unrelated requests from being processed. This issue is fixed in version 4.12.34.	2026-08-07	5.3	CVE-2026-71848
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. From 3.8.0 to 4.12.33, memo() from hono/jsx retains the result of a server side render and reuses it for later renders with comparator equal props, and request scoped values read inside the component take no part in that comparison,	2026-08-07	4.8	CVE-2026-71850

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	so a response can contain HTML rendered for another user's request. Components wrapped with memo() are compared by props alone; values read implicitly during rendering, such as JSX Context through createContext() and useContext(), useRequestContext() from hono/jsx-renderer, and getContext() from hono/context-storage, do not participate, and the retained result lives as long as the wrapped component, so it outlives the request that produced it. A user may receive a response containing HTML rendered for another user when both render the same memoized component with comparator equal props on the same warm instance, which may disclose another user's account or profile data, disclose request scoped secrets embedded in HTML such as CSRF tokens, or expose role specific content to users who should not receive it. This issue is fixed in version 4.12.34.			
Hubzilla--Hubzilla	Hubzilla 11.2.1 contains a cross-site request forgery vulnerability in the OAuth2 /authorize endpoint handled by Zotlabs\Module\Authorize::post() that allows unauthenticated attackers to register arbitrary OAuth2 applications under an authenticated user's account by submitting a cross-origin POST request without CSRF token or Origin/Referer validation. Attackers can craft a malicious HTML form that autosubmits attacker-chosen OAuth2 parameters including client_id, client_secret, redirect_uri, and scope to silently register a persistent OAuth2 application, enabling interception of future OAuth2 authorization codes when the victim later authenticates against the attacker-controlled client.	2026-08-06	4.3	CVE-2026-70556
Hulupeep--mcp-ui-probe	A security flaw has been discovered in Hulupeep mcp-ui-probe up to 0.2.0. Affected is the function get_journey/delete_journey/analyze_journey/usage_stats of the file src/journey/JourneyStorage.ts of the component Journey/Usage. The manipulation of the argument journeyId/filename results in path traversal. The attack requires a local approach. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	5.3	CVE-2026-19270
IBM--Cloud Pak For Business Automation	IBM Cloud Pak For Business Automation 24.0.0, 24.0.1, 25.0.0, and 26.0.0 could allow a remote attacker to obtain sensitive information exposed in manifest files.	2026-08-05	5.3	CVE-2026-12762
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 allows authenticated users can exploit a built-in Langflow component to read arbitrary server environment variables, exposing sensitive secrets despite security controls intended to disable custom components.	2026-08-05	6.5	CVE-2026-10128
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 allows users to read arbitrary files from the server filesystem, including other users' uploaded documents, the JWT signing secret, the SQLite database, and process environment variables, by sending a crafted MCP `resources/read` request with a URL-encoded path traversal sequence in the filename.	2026-08-05	6.5	CVE-2026-7646
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 Langflow could allow server-side request forgery (SSRF) due to incomplete and ineffective SSRF protection enforcement.	2026-08-05	6.5	CVE-2026-7657
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 does not properly validate the username field, allowing attackers to inject path traversal sequences and bypass containment checks. This enables multiple severe impacts, including arbitrary directory deletion, cross-tenant data destruction, and JWT signing key deletion leading to session invalidation.	2026-08-05	6.5	CVE-2026-7658
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 does not properly validate ownership in the deprecated POST /api/v1/build/{flow_id}/vertices endpoint, allowing an authenticated user to inject arbitrary graph data into a shared cache for any flow. This may result in cross-user cache pollution, unauthorized workflow execution, or denial of service.	2026-08-05	5.9	CVE-2026-10547
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.3 is vulnerable to Path Traversal in the Knowledge Bases API (`POST /api/v1/knowledge_bases`). This occurs because user-	2026-08-05	5.4	CVE-2026-7869

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	supplied knowledge base names are used directly to create file paths without proper sanitization or containment checks. An authenticated attacker can exploit this flaw to create directories and write files anywhere on the server's filesystem.			
IBM--Maximo Application Suite	IBM Maximo Application Suite 9.2, 9.1, and 9.0 could allow a remote attacker to tamper with session data due to the use of a weak HMAC session signing secret.	2026-08-05	5.3	CVE-2026-18531
IBM--Maximo Application Suite	IBM Maximo Application Suite 9.2, 9.1, and 9.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	2026-08-05	4.3	CVE-2026-15656
IBM--QRadar	IBM QRadar 7.6.0.0 through 7.6.0.1, and 7.5.0 through 7.5.0 UP 15 Interim Fix 005 could allow an authenticated privileged user to execute arbitrary commands with normal user privileges on the system due to improper validation of user supplied input.	2026-08-05	4.7	CVE-2026-13477
Ichigo3766--image-gen-mcp	A vulnerability was identified in Ichigo3766 image-gen-mcp 0.1.0. The impacted element is an unknown function of the file src/index.ts of the component upscale_images. Such manipulation of the argument output_path leads to path traversal. The attack must be carried out locally. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19365
Simple Membership--Simple Membership	The Simple Membership WordPress plugin before 4.7.7 does not verify that a PayPal payment notification was sent to the site's own configured merchant account before activating a membership, allowing unauthenticated users to activate or extend a membership using a payment made to an arbitrary PayPal account they control.	2026-08-06	5.3	CVE-2026-14936
imranrisal-dev--Student-Management-System	A vulnerability was determined in imranrisal-dev Student-Management-System 18ea7904c339e0c7b0234724a79c939ce6191def/a8d43a29aaf267e7ca97171d6dbb44057bcd7f8c. This affects the function storeProfileImage of the file student_profile_pic.php of the component Shared Upload Helper. Executing a manipulation of the argument choose_file can lead to unrestricted upload. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	6.3	CVE-2026-18927
IncomeStreamSurfer--roo-code-memory-bank-mcp-server	A security vulnerability has been detected in IncomeStreamSurfer roo-code-memory-bank-mcp-server up to 9dcb2fb5e6b65a35ac1983885a6d4e5621a0081e. This affects the function readMemoryBankFile/appendMemoryBankEntry of the file src/index.ts of the component read_memory_bank_file/append_memory_bank_entry. Such manipulation of the argument file_name leads to path traversal. The attack must be carried out locally. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19325
indravoyager--xidown	xidown (a yt-dlp/ffmpeg GUI wrapper) builds its yt-dlp command-line invocation (xidown/core/scanner.py and downloader.py) by appending the user-provided or scanned URL as a bare trailing positional argument, with no '--' end-of-options marker and no scheme validation anywhere in the codebase. Because yt-dlp parses any argument beginning with '-' as a CLI option rather than link text, a crafted 'URL' value such as -U (yt-dlp's self-update flag) or --exec=... is parsed as a real yt-dlp option instead of a URL, altering the tool's control flow before its own URL validation runs. Full code execution via --exec was not demonstrated in the single-URL flow tested, but the underlying argument-injection primitive is confirmed and unmitigated across all call sites.	2026-08-05	4.4	CVE-2026-71212

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IT-Recht Kanzlei--Legal Text Connector of the IT-Recht Kanzlei	Unauthenticated Broken Access Control in Legal Text Connector of the IT-Recht Kanzlei <= 1.0.13 versions.	2026-08-06	6.5	CVE-2026-66452
itsourcecode--Hospital Management System	A weakness has been identified in itsourcecode Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /servicetype.php. This manipulation of the argument editid causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-06	6.3	CVE-2026-19020
itsourcecode--Hospital Management System	A security flaw has been discovered in itsourcecode Hospital Management System 1.0. The affected element is an unknown function of the file /treatment.php. Performing a manipulation of the argument editid results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	2026-08-06	6.3	CVE-2026-19067
itsourcecode--Hospital Management System	A weakness has been identified in itsourcecode Hospital Management System 1.0. The impacted element is an unknown function of the file /treatmentdetail.php. Executing a manipulation of the argument patientid can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-06	6.3	CVE-2026-19068
itsourcecode--Hospital Management System	A security vulnerability has been detected in itsourcecode Hospital Management System 1.0. This affects an unknown function of the file /treatmentrecord.php. The manipulation of the argument editid leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	2026-08-06	6.3	CVE-2026-19069
itsourcecode--Hospital Management System	A vulnerability was detected in itsourcecode Hospital Management System 1.0. This impacts an unknown function of the file /viewadmin.php. The manipulation of the argument delid results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	2026-08-06	6.3	CVE-2026-19070
itsourcecode--Hospital Management System	A flaw has been found in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /viewappointment.php. This manipulation of the argument delid causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	2026-08-06	6.3	CVE-2026-19071
itsourcecode--Hospital Management System	A vulnerability was identified in itsourcecode Hospital Management System 1.0. This issue affects some unknown processing of the file /viewdoctor.php. Such manipulation of the argument delid leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	2026-08-09	6.3	CVE-2026-19347
itsourcecode--Hospital Management System	A vulnerability was determined in itsourcecode Hospital Management System 1.0. The affected element is an unknown function of the file /viewdoctorconsultancycharge.php. This manipulation of the argument delid causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-09	6.3	CVE-2026-19364
Jane-xiaoer--skill-vision-control	A vulnerability has been found in Jane-xiaoer skill-vision-control up to 1.3.0. This vulnerability affects the function getSkillVersionsDir of the file src/svc/utis/config.ts. Such manipulation of the argument skillName leads to path traversal. The attack can only be performed from a local environment. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19335
jeequan--jeepay	A vulnerability was identified in jeequan jeepay up to 3.2.9. This vulnerability affects the function WebSecurityConfig of the file jeepay-manager/src/main/java/com/jeequan/jeepay/mgr/ctrl/sysuser/SysLogController.java of the component PreAuthorize Handler. The manipulation leads to authorization bypass. The attack may be initiated remotely. The exploit is publicly	2026-08-03	6.3	CVE-2026-18631

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.			
Jeff Farthing-- Theme My Login	Unauthenticated Cross Site Request Forgery (CSRF) in Theme My Login <= 7.1.14 versions.	2026-08-06	4.3	CVE-2026-66681
Jevon-Zhong--Ai-doctor	A vulnerability was detected in Jevon-Zhong Ai-doctor 0.0.1. This vulnerability affects the function deleteImage of the file ai-doctor-server/src/filemanagement/filemanagement.service.ts. Performing a manipulation of the argument imagePath results in path traversal. The attack must be initiated from a local position. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	4.4	CVE-2026-19326
jgwhite33--WP TripAdvisor Review Slider	The WP TripAdvisor Review Slider plugin for WordPress is vulnerable to generic SQL Injection via 'curselrevs[]' Parameter in all versions up to, and including, 14.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-05	4.9	CVE-2026-11969
jhy--jsoup	jsoup is a Java library for working with real-world HTML. From 1.14.3 until 1.23.1, jsoup's HTML parser could incorrectly handle a malformed tag name ending in a control character, causing the tag to acquire the parsing behavior of a different element. When a custom Safelist permits certain raw-text elements, this misparsing can cause content that should remain inert text to be emitted as active markup after serialization, potentially resulting in cross-site scripting. jsoup's built-in Safelists are not affected. This issue is fixed in version 1.23.1.	2026-08-06	4.7	CVE-2026-71497
jupyterhub--jupyterhub	JupyterHub is software that allows users to create a multi-user server for Jupyter notebooks. Prior to 5.5.0, invalid input to form-based login authenticators can place an unbounded attacker-controlled username in failed-login logs, allowing an unauthenticated attacker to consume logging and storage resources. This issue is fixed in version 5.5.0.	2026-08-07	5.3	CVE-2026-54338
Justin Kruit--Advanced Custom Fields: Font Awesome Field	Contributor Broken Access Control in Advanced Custom Fields: Font Awesome Field <= 6.1.1 versions.	2026-08-06	4.3	CVE-2026-66678
kalcaddle--kodbox	A flaw has been found in kalcaddle kodbox 1.67 Build 02. This vulnerability affects unknown code of the file /index.php?plugin/msgWarning/action of the component msgWarning Plugin. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	5.3	CVE-2026-18720
kalcaddle--kodbox	A vulnerability has been found in kalcaddle kodbox 1.67 Build 02. This issue affects some unknown processing of the file /user/sso/apiLogin of the component SSO API Login. The manipulation of the argument callbackUrl leads to open redirect. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	4.3	CVE-2026-18721
kata-containers--kata-containers	Kata Containers is an open source implementation of lightweight Virtual Machines (VMs) that perform like containers. In versions prior to 4.0.0, the kata-agent is vulnerable to an authorization bypass in confidential-guest memory management. In Confidential Containers (CoCo) deployments, the kata-agent enforces an OPA/Rego-based AgentPolicy that must authorize every ttRPC API call, forming the security boundary that prevents an untrusted host from directing the confidential guest. Two ttRPC methods introduced with the mem-agent feature are missing this authorization check, so an untrusted host can invoke them unconditionally	2026-08-07	5.7	CVE-2026-64676

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	regardless of the guest's policy configuration. When mem-agent is enabled (off by default), this lets the host tamper with in-guest memory management by forcing swap, aggressive eviction, or compaction, resulting in attacker-controlled availability and performance degradation of the confidential workload entirely outside the agent-policy boundary. The impact does not include memory disclosure or code execution, and severity is bounded by the precondition that mem-agent must be explicitly enabled. This issue is fixed in version 4.0.0.			
Kino-Kafkaesque--ssh-mcp-server	A vulnerability was detected in Kino-Kafkaesque ssh-mcp-server up to 8ebbbb99b26f80ff6162fe00957c6dec73fbc5a5. Impacted is the function ssh_exec of the file src/index.ts of the component SSH Command Handler. Performing a manipulation of the argument host/username results in command injection. The attack requires a local approach. The actual existence of this vulnerability is currently in question. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project maintainer explains: "The intended threat model is that this MCP server is a local/trusted tool for an agent to execute commands over SSH, so callers already have meaningful execution capability through the exposed shell."	2026-08-06	5.3	CVE-2026-19039
Kirachon--context-engine	A vulnerability was determined in Kirachon context-engine up to 1.9.0. This affects the function execGitCommand of the file src/mcp/utis/gitUtils.ts of the component review-git-diff Endpoint. Executing a manipulation of the argument args can lead to command injection. Upgrading to version 1.9.1 mitigates this issue. This patch is called e0729dcfd3a2b1682a7bff86e7174852c03419ba. It is advisable to upgrade the affected component.	2026-08-08	5.5	CVE-2026-19266
klever-io--klever-go	Klever-Go is the Go implementation of the Klever blockchain protocol. In versions prior to 1.7.18, the account-data trie syncers are vulnerable to a resource-exhaustion flaw that leaks bounded throttler slots on error paths. In syncDataTrie() (in both userAccountsSyncer.go and kappAccountsSyncer.go), StartProcessing() reserves a slot from the NumGoRoutinesThrottler, but the corresponding EndProcessing() is only called on the success path and on the duplicate-root early return. As a result, any error from trie.NewTrie(), trie.NewTrieSyncer(), or trieSyncer.StartSyncing() (including the network-dependent timeout path) permanently consumes one slot for the lifetime of the throttler. An attacker who can repeatedly cause trie-node sync failures or timeouts during bootstrap can exhaust the bounded throttler, after which further account-data trie syncs stop making progress and SyncAccounts() returns a timeout. Because epoch bootstrap in syncUserAccountsState() and syncKappAccountsState() aborts on any such error, this causes bootstrap to fail, a core availability issue affecting fresh, restarting, or resyncing nodes and validators. This issue is fixed in version 1.7.18.	2026-08-07	5.9	CVE-2026-49343
KS-GEN-AI--jira-mcp-server	A vulnerability was found in KS-GEN-AI jira-mcp-server 0.2.0. This affects the function axios.get of the file src/index.ts of the component add_attachment_from_public_url. The manipulation of the argument imageUrl results in server-side request forgery. The attack requires a local approach. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19369
kubernetes--Kubernetes	Kubernetes's cluster-controller reconciliation (pkg/utis/clusterclient/clusterclient.go, addCluster) processes every Cluster custom resource's connection configuration and immediately calls Discovery().ServerVersion() against the CRD-specified Kubernetes API endpoint, which is parsed only for URL syntax (url.Parse) with no allow/deny-list for loopback, RFC1918 private ranges, link-local, or cloud-metadata addresses (e.g. 169.254.169.254). A user able to create or update a Cluster CRD can force the controller-manager and apiserver pods to issue outbound requests to arbitrary internal or metadata endpoints.	2026-08-05	6.5	CVE-2026-71208

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
langchain-ai--langgraph	LangGraph Checkpoint Postgres and SQLite Checkpoint are the Postgres and SQLite implementations of LangGraph's checkpoint saver. Prior to 3.1.1, the langgraph-checkpoint-postgres and langgraph-checkpoint-sqlite packages persisted hierarchical namespaces as a dot joined string and scoped reads by matching that string as a simple prefix pattern, so a read scoped to one namespace could also match a sibling namespace whose flattened form shares the same leading characters, or a namespace label containing unescaped pattern metacharacters, allowing an authenticated caller to retrieve stored items belonging to another tenant or user through an ordinary scoped search or list namespaces call, with no crafted input required. This issue is fixed in versions 3.1.1 of langgraph-checkpoint-postgres and langgraph-checkpoint-sqlite.	2026-08-06	5.3	CVE-2026-71433
langchain-ai--langgraphjs	@langchain/langgraph-checkpoint-mongodb provides a LangGraph.js CheckpointSaver implementation that uses MongoDB for storage. Versions 1.3.0 and below are vulnerable to NoSQL injection: checkpoint identifiers (thread_id, checkpoint_ns, checkpoint_id) from config.configurable are passed into MongoDB find() queries in MongoDBSaver.getTuple() without type enforcement. If an attacker supplies an object payload (such as MongoDB operators \$gt or \$ne) instead of a string, it can be interpreted as a query operator, bypassing thread scoping and leaking checkpoints, including pending writes, across tenants. Applications are at risk if they forward untrusted input into config.configurable without coercing it to strings or validating it against a schema, particularly in multi-tenant or user-isolated setups. Apps that only use server-issued, string-typed identifiers with schema validation rejecting non-string fields are not affected. This issue has been fixed in version 1.3.1.	2026-08-04	6.7	CVE-2026-48121
langgenius--dify	A security flaw has been discovered in langgenius dify up to 1.14.2. This issue affects the function jinja2.Template of the file api/core/helper/code_executor/jinja2/jinja2_transformer.py of the component Jinja2 Handler. The manipulation results in improper neutralization of special elements used in a template engine. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	6.3	CVE-2026-18632
latepoint--Appointment Booking Plugin LatePoint Calendar & Scheduling for WordPress	The LatePoint plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'btn_wrapper_classes' attribute of the 'latepoint_resources' shortcode in all versions up to, and including, 5.3.2. This is due to insufficient input sanitization and output escaping in the 'locations' branch of the 'shortcode_latepoint_resources' function. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-06	6.4	CVE-2026-5391
lavkush-maurya--Student-Registration-System	A vulnerability was determined in lavkush-maurya Student-Registration-System 1.0. The affected element is an unknown function of the file /student/changePASS.php. Executing a manipulation of the argument oldpass can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	6.3	CVE-2026-18896
LeeSinLiang--godot-mcp	A flaw has been found in LeeSinLiang godot-mcp 0.1.0. Affected by this vulnerability is the function executeOperation of the file src/index.ts of the component create_scene/add_node. This manipulation of the argument projectPath causes command injection. The attack needs to be launched locally. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	5.3	CVE-2026-19044
Lenovo--XClarity Orchestrator	An improper certificate validation vulnerability was reported in multiple Lenovo XClarity Orchestrator (LXCO) 2.2.0 microservices that could allow an adjacent network attacker to intercept sensitive communications by performing a machine-	2026-08-04	6.1	CVE-2026-16792

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in-the-middle attack against HTTPS connections during TLS certificate validation under certain circumstances.			
litestar-org-- litestar	Litestar is an Asynchronous Server Gateway Interface (ASGI) framework. In versions prior to 2.22.0, an attacker can bypass the allowed hosts validation by omitting the Host header and supplying an X-Forwarded-Host header set to a whitelisted domain. The AllowedHostsMiddleware trusts the X-Forwarded-Host header as a fallback when the Host header is absent. Since X-Forwarded-Host is a client-controllable header, this enables host header injection attacks such as password reset poisoning, cache poisoning, and server-side request routing manipulation. Any application using AllowedHostsConfig is affected when deployed without a reverse proxy that strips X-Forwarded-Host, or when accepting HTTP/1.0 connections. This issue has been fixed in version 2.22.0.	2026-08-03	5.9	CVE-2026-48061
Imammino--oidc- authorizer	A vulnerability has been found in Imammino oidc-authorizer 0.4.0. This issue affects the function parse_token_from_header of the file src/parse_token_from_header.rs of the component Authorization Header Parsing. The manipulation of the argument authorization_token leads to denial of service. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-09	5.3	CVE-2026-19362
Imammino--oidc- authorizer	A vulnerability was found in Imammino oidc-authorizer up to 0.4.0. Impacted is an unknown function of the file src/handler.rs of the component Lambda Authorizer. The manipulation results in sensitive information in log files. The attack can be executed remotely. `src/handler.rs` logs raw Authorization header values and complete bearer tokens/JWTs on authentication failure paths, potentially exposing credentials through CloudWatch Logs. `src/models.rs` serializes the complete validated JWT claims set with `serde_json::to_string(token_claims).unwrap()` and propagates it through `context["jwtClaims"]` to downstream integrations. This code performs serialization, not deserialization, and does not process attacker-controlled `jwtClaims` input. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-09	5.3	CVE-2026-19363
lock-upme--OPMS	A vulnerability was found in lock-upme OPMS up to 831440f37a92c1568f2e071d5233bc873a9d8b09. The impacted element is an unknown function of the file controllers/messages/message.go of the component IN Clause Handler. Performing a manipulation of the argument ids results in sql injection. The attack is possible to be carried out remotely. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-09	6.3	CVE-2026-19354
Logo Software Industry and Trade Inc.--e-Logo Purchasing Portal	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Logo Software Industry and Trade Inc. E-Logo Purchasing Portal allows Stored XSS. This issue affects e-Logo Purchasing Portal: before 1.52.	2026-08-06	5.4	CVE-2026-8166
Lspace-io--Lspace- server	A vulnerability was detected in Lspace-io Lspace-server up to 79f02fe5aa8970b210a6a05cf097155f8d9ffd71. This issue affects the function fileExists/readFile/writeFile/deleteFile of the file src/core/repository.ts of the component Repositories File API. Performing a manipulation of the argument filePath results in path traversal. The attack is only possible with local access. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	5.3	CVE-2026-19054
marimo-team-- marimo	marimo before 0.23.15 contains a configuration injection vulnerability that allows notebook authors to exfiltrate operator API keys by embedding a malicious base_url in PEP-723 inline script metadata, which is merged into session	2026-08-04	6.5	CVE-2026-67618

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configuration with higher precedence than the operator's own settings due to insufficient sanitization in sanitize_pyproject_dict. When an operator opens the crafted notebook and makes an AI request, marimo resolves the attacker-controlled base_url from the notebook config while falling back to the operator's OPENAI_API_KEY environment variable for authentication, transmitting the API key to the attacker-controlled endpoint without requiring any cell execution.			
Mark Jaquith-- Subscribe to Comments	Author Cross Site Scripting (XSS) in Subscribe to Comments <= 2.3.1 versions.	2026-08-06	5.9	CVE-2026-66706
MauricioMilano-- coder-api	A security vulnerability has been detected in MauricioMilano coder-api up to 1.1.0. Affected is the function createProject of the file src/core/projects.ts of the component Projects Endpoint. The manipulation leads to command injection. The attack must be carried out locally. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	5.3	CVE-2026-19284
maximeAmini-- Atals-Livre	Atals-Livre contains a SQL injection vulnerability that allows attackers to manipulate database queries by passing unsanitized input through a GET parameter to the supp() deletion helper function. Attackers can inject malicious SQL syntax via the vulnerable GET parameter to perform unauthorized database operations including data deletion and extraction.	2026-08-04	6.5	CVE-2026-69704
mealie-recipes-- mealie	Mealie's AsyncSafeTransport SSRF guard (mealie/pkgs/safehttp/transport.py) resolves a target hostname once, checks the resolved IP against private-range rules, but then issues the actual outbound HTTP request using the original hostname, which the underlying async transport re-resolves independently. Because the validated IP is never pinned to the actual connection, a DNS-rebinding attacker (returning a public IP to the validation lookup and a private/metadata IP to the real connection) defeats the guard. This is reachable by any authenticated user via /api/recipes/create/url, /api/recipes/test-scraper-url, and /api/recipes/{slug}/image, and the scraper reflects fetched content back to the requester, allowing an authenticated user to read internal HTTP services and cloud-metadata endpoints.	2026-08-05	5.3	CVE-2026-71210
Medixant--RadiAnt DICOM	Opening a crafted DICOM file containing malicious JPEG-compressed pixel data triggers an attacker-controlled heap out-of-bounds write, which may allow an attacker to remotely execute arbitrary code.	2026-08-06	4.3	CVE-2026-17264
Mercado Pago-- Mercado Pago payments for WooCommerce	Unauthenticated Insecure Direct Object References (IDOR) in Mercado Pago payments for WooCommerce <= 8.9.0 versions.	2026-08-06	5.3	CVE-2026-28180
metaslider--Slider, Gallery, and Carousel by MetaSlider Image Slider, Video Slider	The Slider, Gallery, and Carousel by MetaSlider - Image Slider, Video Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'delay' Post Meta Setting in all versions up to, and including, 3.111.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The ml-slider custom post type is registered without custom capability restrictions and the ml-slider_settings meta key is unprotected, allowing Author-level users to set the malicious delay value via XML-RPC custom_fields when creating an ml-slider post.	2026-08-06	6.4	CVE-2026-18400
mf-yang-- openclaw-cn	A vulnerability was found in mf-yang openclaw-cn 2026.2.5. This affects an unknown part of the file src/agents/bash-tools.exec.ts of the component Ggateway Exec Approval Flow. The manipulation results in incorrect authorization. The attack may be performed from remote. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	6.3	CVE-2026-19006

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mf-yang--openclaw-cn	A vulnerability was determined in mf-yang openclaw-cn up to 0.2.1. This vulnerability affects the function isApprovedElevatedSender of the file src/auto-reply/reply/reply-elevated.ts. This manipulation causes improper privilege management. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	6.3	CVE-2026-19007
mf-yang--openclaw-cn	A vulnerability was identified in mf-yang openclaw-cn up to 0.2.1. This issue affects the function assertNoSymlinkEscape of the file src/agents/sandbox-paths.ts of the component apply_patch Tool. Such manipulation leads to link following. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	6.3	CVE-2026-19008
Microsoft--Microsoft Edge (Chromium-based)	Improper control of generation of code ('code injection') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-08-03	6.1	CVE-2026-65804
Microsoft--Microsoft Edge (Chromium-based)	Missing authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform tampering locally.	2026-08-03	6.2	CVE-2026-66311
Microsoft--Microsoft Edge (Chromium-based)	Buffer over-read in Microsoft Edge (Chromium-based) allows an authorized attacker to execute code over a network.	2026-08-03	6.5	CVE-2026-66312
Microsoft--Microsoft Edge (Chromium-based)	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform tampering locally.	2026-08-03	6.8	CVE-2026-66313
Microsoft--Microsoft Edge (Chromium-based)	Time-of-check time-of-use (toctou) race condition in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2026-08-03	6.5	CVE-2026-66314
Microsoft--Microsoft Edge (Chromium-based)	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-08-03	6.1	CVE-2026-66325
Microsoft--Microsoft Edge (Chromium-based)	Missing authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-08-03	6.5	CVE-2026-66326
Microsoft--Microsoft Edge (Chromium-based)	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-08-03	5.4	CVE-2026-66316
Microsoft--Microsoft Edge (Chromium-based)	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform tampering over a network.	2026-08-03	5.4	CVE-2026-66317
microweber--microweber	Microweber CMS through 2.0.20 contains a stored cross-site scripting vulnerability in the content tagging system that allows admin-authenticated attackers to inject arbitrary JavaScript by submitting malicious payloads via the tag_names parameter of the GET /api/save_content_admin endpoint, bypassing three independent sanitization controls including XSS middleware that ignores GET requests, a strip_unsafe() function that only matches double-quoted onerror attributes, and a titlecase normalizer that passes HTML decimal entity-encoded payloads through unchanged. Attackers can store malicious scripts that execute without user interaction for every visitor to the public blog page and within the admin post editor, enabling session riding through same-origin fetch requests using the CSRF token embedded in the page.	2026-08-03	4.8	CVE-2026-67617

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
miguelsobain--ember-dynamic-render-template	The render-template component of ember-dynamic-render-template (addon/components/render-template.js) passes its `templateString` property directly into Ember/Glimmer's compileTemplate() (from @ember/template-compilation) with no sanitization, allow-listing, or validation of the input. Because compileTemplate() dynamically compiles and renders the supplied string as a live Handlebars/Glimmer template, any application that renders attacker-influenced data through this component's templateString property is exposed to client-side template injection: an attacker-controlled Handlebars expression is compiled and executed in the context of the rendering component, which can be leveraged for cross-site scripting depending on what helpers/context are exposed to the compiled template.	2026-08-05	6.1	CVE-2026-71286
MIMICLab--mcp-pdf-vision	A vulnerability was identified in MIMICLab mcp-pdf-vision 1.1.0. The impacted element is the function load_pdf of the file src/index.ts. Such manipulation of the argument pdfPath/sessionId leads to command injection. The attack can only be performed from a local environment. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	5.3	CVE-2026-19279
MingSoft--MCMS	A vulnerability was identified in MingSoft MCMS up to 3.0.6. This impacts an unknown function of the file /mdiy/form/data/list of the component ms-mdiy. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-09	5.3	CVE-2026-19356
MingSoft--MCMS	A security flaw has been discovered in MingSoft MCMS up to 3.0.6. Affected is an unknown function of the file /mdiy/form/get of the component ms-mdiy. The manipulation results in information disclosure. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-09	5.3	CVE-2026-19357
MissionSquad--mcp-api	A flaw has been found in MissionSquad mcp-api up to 1.11.9. The affected element is an unknown function of the file src/services/dcrClients.ts. Executing a manipulation can lead to server-side request forgery. The attack may be performed from remote. Upgrading to version 1.11.10 is sufficient to fix this issue. This patch is called f068ab4ad6f0907ac7001b995588c2673f11a755. You should upgrade the affected component.	2026-08-06	6.3	CVE-2026-19040
MissionSquad--mcp-api	A vulnerability has been found in MissionSquad mcp-api up to 1.11.8. The impacted element is the function this.packageService.installPackage of the file src/controllers/packages.ts of the component NPM Package Version Handler. The manipulation leads to command injection. It is possible to initiate the attack remotely. Upgrading to version 1.11.9 is sufficient to resolve this issue. The identifier of the patch is a40f54d4533ba6618e1749383a245900eeb024c1. The affected component should be upgraded.	2026-08-06	6.3	CVE-2026-19041
Mobi-Com Polska Sp. z o.o.--stunnel	A stack-based out-of-bounds read vulnerability exists in the "s_vlog" function of stunnel, when handling oversized log messages via "vsprintf". A remote attacker with network access to a stunnel service can send protocol inputs that trigger a log message longer than 1024 bytes, leading to an out-of-bounds stack read and a potential crash. In certain corner cases, the same vulnerability could be used to replace a series of trailing "\n" characters with "\0".	2026-08-04	6.5	CVE-2026-70368
Mobi-Com Polska Sp. z o.o.--stunnel	A Server-Side Request Forgery (SSRF) bypass vulnerability exists in "stunnel" 5.79 and lower when configured in SOCKS proxy mode. This flaw allows a client to bypass intended localhost restrictions by using IPv4-mapped IPv6 addresses (e.g., "::ffff:127.0.0.1") or unspecified addresses ("0.0.0.0", ":::"), enabling access to loopback-only services on the "stunnel" host that should not be network-reachable.	2026-08-04	5.4	CVE-2026-70367

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MonomythDevelopment--la-forge-mcp	A security vulnerability has been detected in MonomythDevelopment la-forge-mcp 1.0.0. This issue affects the function screenshotElement of the file src/index.ts of the component screenshot_element Tool. Such manipulation of the argument output_name leads to path traversal. The attack can be executed remotely. Upgrading to version 1.1.1 is capable of addressing this issue. The name of the patch is 1102172c9adec4a619e241efd6bfb74f5b1f4332. Upgrading the affected component is advised. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-08-06	6.3	CVE-2026-19038
MZ Automation--libiec61850	A vulnerability was found in MZ Automation libiec61850 up to 1.6.1. The affected element is the function deleteDataSetValuesShadowBuffer of the file src/iec61850/server/mms_mapping/reporting.c of the component URCB Revalidation. The manipulation results in use after free. The attack needs to be approached locally. The exploit has been made public and could be used. Upgrading to version 1.6.2 is sufficient to fix this issue. The patch is identified as 486fd57f3aed65bb9d636ff00f9ddce2e450b168. Upgrading the affected component is advised.	2026-08-06	5.3	CVE-2026-19108
MZ Automation--libiec61850	A security flaw has been discovered in MZ Automation libiec61850 up to 1.6.1. This affects the function SVReceiver_stopThreadless of the file src/sampled_values/sv_subscriber.c of the component ASDU Element Handler. Performing a manipulation results in heap-based buffer overflow. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. Upgrading to version 1.6.2 is able to mitigate this issue. The patch is named a96bd674e0238276dd1387d31d52e55229d0771e. The affected component should be upgraded.	2026-08-07	5.3	CVE-2026-19206
MZ Automation--libiec61850	A vulnerability has been found in MZ Automation libiec61850 up to 1.6.1. The affected element is the function MmsMapping_varAccessSpecToObjectReference of the file src/iec61850/common/iec61850_common.c of the component MMS Protocol Workflow. Such manipulation of the argument GetNamedVariableListAttributesResponse.itemId leads to heap-based buffer overflow. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-08	5.3	CVE-2026-19259
mz-automation--libiec61850	A security flaw has been discovered in mz-automation libiec61850 up to 1.6.1. This vulnerability affects the function Reporting_RCBWriteAccessHandler of the file src/iec61850/server/mms_mapping/reporting.c of the component Report Sending Path Handler. The manipulation results in free of memory not on the heap. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 1.6.2 is able to resolve this issue. The patch is identified as 5b2a69f44256b8548927d8afdd7ac5f5381abe1e. It is suggested to upgrade the affected component. The vendor was contacted early about this disclosure.	2026-08-03	5.3	CVE-2026-18582
mz-automation--libiec61850	A weakness has been identified in mz-automation libiec61850 up to 1.6.1. This issue affects the function checkDataSetAccess of the file src/iec61850/server/mms_mapping/mms_mapping.c of the component MMS Request Handler. This manipulation causes out-of-bounds read. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 1.6.2 is capable of addressing this issue. Patch name: 062062daf4cb50c7aa76e01d6fb4d58fc9278a7d. Upgrading the affected component is recommended. The vendor was contacted early about this disclosure.	2026-08-03	5.3	CVE-2026-18583
nanocoai--NanoClaw	A vulnerability was detected in nanocoai NanoClaw up to 2.0.64. Affected is the function handleCreateAgent of the file src/modules/agent-to-agent/create-agent.ts of the component Child-Agent Creation. Performing a manipulation results in improper privilege management. Remote exploitation of the attack is possible.	2026-08-06	6.3	CVE-2026-19005

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.			
nearai--ironclaw	A vulnerability was identified in nearai ironclaw up to 0.29.1. Affected is the function <code>classify_command_risk</code> of the file <code>src/tools/builtin/shell.rs</code> . Such manipulation leads to command injection. The attack may be launched remotely. The exploit is publicly available and might be used. The name of the patch is <code>a1d7c3ba428ed575900469b207fb5668725f9a71</code> . Applying a patch is advised to resolve this issue.	2026-08-06	6.3	CVE-2026-18980
NellyW8--MCP4EDA	A security vulnerability has been detected in NellyW8 MCP4EDA 1.0.0. Affected by this vulnerability is an unknown functionality of the component <code>run_openlane/view_waveform</code> . The manipulation of the argument <code>design_name/vcd_file</code> leads to command injection. Local access is required to approach this attack. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19332
netease-youdao--LobsterAI	A flaw has been found in netease-youdao LobsterAI 2026.6.10. This affects the function <code>parseMediaTokensFromText</code> of the file <code>src/renderer/services/artifactParser.ts</code> of the component MEDIA Path Handler. This manipulation causes information disclosure. The attack is possible to be carried out remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	4.3	CVE-2026-18995
netty--netty	Netty is an asynchronous, event-driven network application framework. Prior to 4.1.136.Final and 4.2.16.Final, the <code>RedisArrayAggregator</code> Redis codec clears retained partial aggregate state when the <code>maxNestedArrayDepth</code> limit is exceeded, but it does not clear the same state when the sibling <code>maxElements</code> limit is exceeded. A peer can start a valid RESP array, send a bulk string child, then send a nested array header longer than the configured <code>maxElements</code> . Netty throws a decoder exception in <code>decodeRedisArrayHeader</code> , but the existing partial aggregate remains retained in the handler. If the application leaves the channel alive after the exception, later messages are still consumed into the pre-error aggregate, allowing an unauthenticated peer to keep attacker-controlled aggregate state alive across a security-limit exception and pin retained pooled buffers. This issue is fixed in versions 4.1.136.Final and 4.2.16.Final.	2026-08-07	6.5	CVE-2026-56818
NewType--WebEIP	A vulnerability was detected in NewType WebEIP up to 3.0. This affects an unknown part of the file <code>/EIP_Com_FileList.aspx</code> . The manipulation results in improper authentication. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	5.3	CVE-2026-18610
Nexcess--Gutenberg Blocks by Kadence Blocks	Contributor Sensitive Data Exposure in Gutenberg Blocks by Kadence Blocks <= 3.7.8 versions.	2026-08-06	4.3	CVE-2026-66696
NightTrek--Ollama-mcp	A flaw has been found in NightTrek Ollama-mcp up to <code>80cf2e17cfc144963a475b619093a2d13c13dbc9</code> . This affects an unknown part of the file <code>src/index.ts</code> . This manipulation of the argument <code>name/modelfile/source/destination</code> causes command injection. The attack can only be executed locally. This product is using a rolling release to provide continuous delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19334
NightTrek--Supabase-MCP	A vulnerability was detected in NightTrek Supabase-MCP <code>cc994ab2d2a36b0af6ee7c7f3e6ce8e08cda2170/db03237d92f7dc2f0da0d70a87dba84ebcde5b66</code> . Affected by this issue is some unknown functionality of the component <code>generate_types</code> . The manipulation of the argument schema results in	2026-08-09	5.3	CVE-2026-19333

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	command injection. The attack needs to be approached locally. The project was informed of the problem early through an issue report but has not responded yet.			
Nikolaibibo-- claude-comfyui-mcp	A vulnerability was identified in Nikolaibibo claude-comfyui-mcp 1.0.0. Affected is the function copyFileSync of the file src/tools/utlis.ts of the component comfy_upload_image. Such manipulation of the argument image_path leads to path traversal. An attack has to be approached locally. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19371
Ninja Forms--Ninja Forms	The Ninja Forms WordPress plugin before 3.14.10 does not prevent user-supplied query-string input, used to pre-populate a form field's default value, from being processed as a shortcode, allowing unauthenticated attackers to execute arbitrary shortcodes registered on the site when a form so configured is embedded on a public page.	2026-08-06	4.8	CVE-2026-15256
NocteDefensor-- LudusMCP	A vulnerability has been found in NocteDefensor LudusMCP 1.0.24. Affected by this vulnerability is an unknown functionality of the file src/tools/rangeConfig.ts of the component read_range_config. The manipulation of the argument Source leads to server-side request forgery. The attack may be initiated remotely. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	6.3	CVE-2026-19367
NocteDefensor-- LudusMCP	A weakness has been identified in NocteDefensor LudusMCP up to 1.0.24. The affected element is the function SecretDialog.showSecretDialog of the file src/utlis/secretDialog.ts of the component get_credential_from_user. This manipulation of the argument Description causes command injection. It is possible to launch the attack on the local host. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	5.3	CVE-2026-19045
NocteDefensor-- LudusMCP	A vulnerability was detected in NocteDefensor LudusMCP up to 1.0.24. This affects the function executeArbitraryCommand/executeCommand of the file src/ludusMCP/cliWrapper.ts of the component ludus_cli_execute. Performing a manipulation of the argument command/args results in command injection. The attack needs to be approached locally. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	5.3	CVE-2026-19047
NocteDefensor-- LudusMCP	A flaw has been found in NocteDefensor LudusMCP up to 1.0.24. Affected is an unknown function of the file src/tools/insertCredsRangeConfig.ts of the component insert_creds_range_config. Executing a manipulation of the argument configPath/outputPath can lead to path traversal. The attack is restricted to local execution. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19366
NousResearch-- hermes-agent	A vulnerability was detected in NousResearch hermes-agent up to 2026.6.5. Affected by this issue is the function _check_slash_access of the file gateway/run.py of the component Quick Command Handler. The manipulation results in incorrect authorization. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	6.3	CVE-2026-18773
NousResearch-- hermes-agent	A flaw has been found in NousResearch hermes-agent up to 0.16.0. This affects the function save_url_image of the file agent/image_gen_provider.py of the component xAI Image Generation Provider. This manipulation causes server-side request forgery. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	6.3	CVE-2026-18774
NousResearch-- hermes-agent	A vulnerability has been found in NousResearch hermes-agent up to 0.16.0. This vulnerability affects the function browser_snapshot of the file tools/browser_tool.py of the component Browser Tooling. Such manipulation leads to server-side request forgery. The attack may be launched remotely. The exploit	2026-08-04	6.3	CVE-2026-18775

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
NousResearch--hermes-agent	A vulnerability was determined in NousResearch hermes-agent up to 0.16.0. This impacts the function get_tool_definitions of the file agent/agent_init.py of the component disabled_toolsets Handler. This manipulation causes incorrect privilege assignment. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report.	2026-08-06	6.3	CVE-2026-18976
NousResearch--hermes-agent	A vulnerability was detected in NousResearch hermes-agent up to 0.16.0. Affected by this issue is some unknown functionality of the file hermes-agent/model_tools.py of the component Memory Toolset. The manipulation results in improper access controls. The attack can be executed remotely. The exploit is now public and may be used.	2026-08-06	6.3	CVE-2026-18993
nuxt--nuxt	Nuxt is an open-source web development framework for Vue.js. From 3.1.0 until 3.21.10 and 4.5.1, an attacker can supply a top-level `as` prop to the /__nuxt_island/ endpoint and drive dynamic component resolution through <component :is>, resolveDynamicComponent, or h(). This issue is fixed in 3.21.10 and 4.5.1.	2026-08-05	4.8	CVE-2026-71318
NVIDIA--Dynamo	NVIDIA Dynamo for Linux examples and recipes contain a vulnerability where an attacker could cause a system failure. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, and information disclosure.	2026-08-04	6.6	CVE-2026-47619
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause a race condition in the LoRA manager singleton initialization. A successful exploit of this vulnerability might lead to data tampering and denial of service.	2026-08-04	6.5	CVE-2026-47620
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause a race condition in the LoRA manager singleton initialization. A successful exploit of this vulnerability might lead to denial of service and data tampering.	2026-08-04	6.5	CVE-2026-47621
NVIDIA--Dynamo	NVIDIA Dynamo for Linux contains a vulnerability where an attacker could cause the generation of error messages that contain sensitive information. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-04	5.3	CVE-2026-47622
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where a user could cause files outside the model repository to be read, written to, or modified by providing a path in the model name to the Triton MLflow plugin. A successful exploit of this vulnerability might lead to denial of service and information disclosure.	2026-08-04	4.4	CVE-2026-47487
nxp-auto-goldvip--gvip	A security vulnerability has been detected in nxp-auto-goldvip gvip up to 1.4.0. Affected by this issue is the function SitewiseCustomFunction of the component Lambda Function Handler. Such manipulation leads to improper access controls. The attack can be launched remotely. Upgrading to version 1.15.0 can resolve this issue. Upgrading the affected component is advised. The project explains: "The reported IAM permission configuration is a known historical issue that was already addressed in 2024, beginning with GoldVIP version 1.13.0. The permissions were updated in subsequent releases, including version 1.15.0. In addition, we also sent a request to either update or deprecate the older release in the AWS SAR application repository."	2026-08-09	4.7	CVE-2026-19359
o6--open62541	A vulnerability was found in o6 open62541 up to 1.5.5. This issue affects the function UA_Client_readNodeClassAttribute of the file src/client/ua_client_highlevel.c. Performing a manipulation results in heap-based buffer overflow. Attacking locally is a requirement. The exploit has been made	2026-08-04	5.3	CVE-2026-18784

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	public and could be used. The project closed the issue report, stating that this is not the official way to report a security vulnerability.			
o6--open62541	A vulnerability was determined in o6 open62541 ca356b088ada7dee824d1b4acd07c1ff07ce242b. Impacted is the function UA_Client_getRemoteDataTypes of the file examples/custom_datatype/client_types_custom.c. Executing a manipulation can lead to use after free. It is possible to launch the attack on the local host. The exploit has been publicly disclosed and may be utilized. The project closed the issue report, stating that this is not the official way to report a security vulnerability.	2026-08-04	5.3	CVE-2026-18785
odysseus-dev--odysseus	Odysseus before commit 87babb5 contains a server-side request forgery vulnerability that allows admin-privileged attackers to direct the server to probe internal network resources by supplying arbitrary URLs to the embedding endpoint configuration without scheme, host, IP range, or DNS rebind validation. Attackers can submit loopback addresses, RFC 1918 ranges, or link-local addresses through the embedding endpoint API to partially read responses from cloud instance metadata services, internal APIs, and other hosts reachable from the server.	2026-08-04	6.8	CVE-2026-70620
OMICRON electronics GmbH--OMICRON StationGuard	OMICRON StationGuard 4.00 contains an improper input validation vulnerability in its IEC 61850 Sampled Values (SV) frame processing. A specially crafted SV frame can cause the affected process to terminate, disrupting alert processing for Sampled Values traffic. The vulnerability does not affect overall system availability or the processing of other traffic types, and the process is automatically restarted, and the failure is immediately reported to the user.	2026-08-06	4.3	CVE-2026-16316
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.5, the `add-to-tunnel` endpoint creates a new appointment row in any client tunnel without any caller authentication. A request that supplies any valid `tunnelId` and any valid `emailHash` (the two need not belong to the same tunnel) results in an inserted appointment with `status = "CONFIRMED"`, attacker-controlled ciphertext fields, attacker-controlled date and duration, and an attacker-chosen agent. The endpoint validates only that some tunnel exists with the given `emailHash`, then writes the appointment using the attacker-supplied `tunnelId` directly. The `emailHash` lookup is effectively an existence check on the tenant; it does not authenticate the caller as the owner of the supplied `tunnelId`. Combined with the absence of any session, Authorization header, booking access token, or PoW, this makes the endpoint accept arbitrary appointment writes into arbitrary tunnels. By contrast, the sibling endpoint `create-new-client` (used to bootstrap a brand-new client tunnel) requires a Bearer bootstrap booking access token issued by the bootstrap-challenge / bootstrap-verify flow. The `add-to-tunnel` endpoint, intended for return-clients booking additional appointments, has no equivalent gate. The application's own middleware confirms this is intentional: `add-to-tunnel` is explicitly listed in the apiAuthHandle public-route allowlist alongside the bootstrap and challenge endpoints (which legitimately have no session). Version 1.0.5 fixes the issue.	2026-08-06	6.5	CVE-2026-48075
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. The new-client booking flow in versions 1.0.1 and prior consists of three calls: `bootstrap-challenge` (returns a 16-bit PoW challenge with `difficulty=4` leading hex zeroes), `bootstrap-verify` (validates the PoW and issues a Bearer booking access token), and `create-new-client` (consumes the token and creates the tunnel and first appointment). The token correctly binds to `tenantId`, `tunnelId`, `clientPublicKey`, and `emailHash`, but never to `channelId`. The `bootstrap-challenge` request schema does not even accept a `channelId`, and the issued token's payload contains no channel information. Independently, the service function `createNewClientWithAppointment` checks only `channel.archived = false`. The `channel.isPublic` check that protects `addAppointmentToTunnel` is missing in the new-client path. The combination means: an attacker completes the	2026-08-06	6.5	CVE-2026-48076

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bootstrap flow normally (16-bit PoW, completes in well under one second on commodity hardware, no rate limiting beyond the throttle store), receives a valid booking access token, and then submits the `create-new-client` payload with `channelId` pointing to a private (`isPublic = false`) channel. The booking lands as `CONFIRMED` if the target channel has `requiresConfirmation = false` (the default), otherwise as `NEW`. The patient-facing UI does not list private channels in its picker (`/api/public/channels` correctly filters `isPublic = true`), so the channel ID must be obtained out of band. The companion finding V-10 (schedule endpoint discloses private channels) provides exactly that: a single unauthenticated GET reveals every private channel ID for any tenant. V-10 plus V-11 together make private channels fully reachable to anonymous attackers. As of time of publication, no known patched versions are available.			
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.2, the `/api/log` endpoint accepts unauthenticated POST requests, applies no schema validation to the message body, writes attacker-controlled content directly into the application's stdout log, interprets newline characters as real line breaks, and enforces no size or rate limits. Three independent abuse modes follow: log injection (forge log lines that look like legitimate system events), log volume DoS (saturate the logging pipeline at sustained 100+ requests per second of small messages), and oversized-payload submission (100 KB payloads accepted; larger sizes not tested). The most operationally damaging mode is log injection. An attacker can inject lines that an operator scanning logs would mistake for real system errors, mask their own activity behind fake noise, or pollute SIEM alerting rules with crafted false positives. A line such as `[error]: injected admin error` injected from an unauthenticated source is indistinguishable from the application's own error output once written to disk. Version 1.0.2 fixes the issue.	2026-08-06	6.5	CVE-2026-48083
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.4, the PIN-type challenge throttle uses `emailHash` as the only key. The throttle rows live in the central `challenge_throttle` table, which is shared across all tenants. Every tenant's `/api/tenants/{id}/appointments/verify-challenge` endpoint increments the same row when a PIN response fails, and every tenant's `/api/tenants/{id}/appointments/challenge` endpoint reads the same row when deciding whether to issue a new challenge. When the same `emailHash` exists in multiple tenants on the same OpenReception instance (the same patient holding tunnels in two different clinics that share the platform), an attacker who knows the patient's email can lock out that patient on tenant B by issuing failed challenge responses against tenant A. The attacker needs no relationship to tenant B; the lockout propagates through the shared throttle row. The lockout escalates with repeated failures. The first lockout triggers at 4 failed attempts and lasts approximately 60 seconds. Subsequent failures escalate the lockout duration to 5 minutes, 30 minutes, and 60 minutes per the throttle service's escalation logic. Repeated bursts produce sustained denial of service against the targeted email. Version 1.0.4 patches the issue.	2026-08-06	5.8	CVE-2026-48071
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.1.0, the GET handler at `/api/tenants/{id}/appointments/{appointmentId}` performs no authorization check before returning the appointment record. Any party who knows or obtains a valid appointment UUID receives the full row, including channel and agent IDs, time and timezone, status, and the AES-GCM ciphertext components (`encryptedPayload`, `iv`, `authTag`, `dataKey`). The same file's DELETE handler calls `checkPermission(locals, tenantId, true)` before allowing deletion. The intent is clear: appointment records are tenant-scoped and require authentication to access. The GET handler is missing the equivalent call. The middleware chain (`apiAuthHandle`, `authGuard`) does not compensate: API paths bypass	2026-08-06	5.3	CVE-2026-48077

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`authGuard` entirely, and `apiAuthHandle` does not block requests to non-admin paths when no token is present. Version 1.1.0 patches the issue.			
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.5, the unauthenticated `/api/tenants/{id}/schedule` endpoint returns every non-archived channel for a tenant regardless of the channel's `isPublic` flag. Channels marked `isPublic = false` are intended to be invisible to public callers; the dashboard creates them deliberately to hide internal-only services from the patient booking UI. The schedule endpoint ignores the flag entirely and discloses channel names, descriptions, IDs, agent associations, pause status, confirmation requirements, and computed slot availability for the requested date range. The asymmetry between `addAppointmentToTunnel` (which enforces `eq(channel.isPublic, true)`) and the schedule endpoint (which does not) confirms the design intent: private channels exist as a real access boundary in the booking flow, just not in the schedule disclosure. Version 1.0.5 patches the issue.	2026-08-06	5.3	CVE-2026-48078
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. Prior to 0.11.0, Open WebUI resolved a hostname during URL validation and rejected private, loopback, and link-local addresses, but the HTTP clients resolved the hostname again at connection time. An authenticated attacker who controlled authoritative DNS for a submitted hostname could answer with a public address during validation and an internal one during connection, reaching cloud metadata, loopback admin APIs, or internal services through URL ingest, chat image_url fetches, image editing, or OAuth profile-picture fetches, with most paths returning the response to the attacker and the OAuth path forwarding the OAuth access token. This issue is fixed in 0.11.0.	2026-08-04	6.3	CVE-2026-54020
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.0 until 0.11.0, automation recurrence parsing in backend/open_webui/utils/automations.py anchored minutely and hourly rules at a fixed date of 2000-01-01 and then walked forward one interval at a time to find the next run. A single FREQ=MINUTELY rule enumerates roughly a quarter-century of occurrences synchronously on the event loop that also serves scheduler, HTTP, and WebSocket traffic, and the scheduler recomputes the next run for every claimed row on each poll. This causes availability impact for every other user of the instance. This issue is fixed in 0.11.0.	2026-08-04	6.5	CVE-2026-70489
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.8 until 0.11.0, the terminal WebSocket route in backend/open_webui/routers/terminals.py authenticated its own first-message JWT and never applied the verified-user role gate that get_verified_user enforces on HTTP terminal routes. An account whose role is pending, including a registered but unapproved account or an account deactivated back to pending, can open an interactive terminal session when at least one terminal server is configured and its access grants cover the account. This loses the account-approval boundary for terminal access while the HTTP terminal routes correctly reject the same account. This issue is fixed in 0.11.0.	2026-08-04	6.3	CVE-2026-70490
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. In 0.10.2 and earlier, the GET /api/v1/tools/, GET /api/v1/tools/list, and GET /api/v1/tools/{id} endpoints in backend/open_webui/routers/tools.py returned full Python tool source to authenticated non-admin read-only users. ToolResponse deliberately omitted source and specs, but ToolUserResponse permitted extra fields and handlers spread a full tool model dump into the response, re-admitting omitted fields. A non-admin with a read grant can obtain another user's server-side tool source, which commonly embeds hard-coded API keys, credentials, and internal service URLs. This issue is fixed in 0.11.0.	2026-08-04	6.5	CVE-2026-70491

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 until 0.11.0, the built-in knowledge search path in backend/open_webui/tools/knowledge_fs.py and backend/open_webui/tools/builtin.py let a chat participant choose a pattern used to grep knowledge files. Patterns containing regex metacharacters were compiled with Python's backtracking re engine and run against every line of every reachable file with no time limit, so a crafted pattern such as (x x)*y and one matching uploaded file line can pin one CPU core and block the event loop. This causes availability impact for every other user of the affected worker. This issue is fixed in 0.11.0.	2026-08-04	6.5	CVE-2026-70493
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.5.0 until 0.11.0, the standard channel message update and delete handlers accepted any caller holding write access on the channel without checking that the caller wrote the message. Because write access is the same grant a member needs to post, any ordinary participant in a shared standard channel could rewrite or permanently delete another participant message, while group and direct message handlers enforced authorship. This issue is fixed in 0.11.0.	2026-08-04	5.4	CVE-2026-70481
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.8.8 until 0.11.0, inline direct model metadata accepted client-supplied knowledge attachments without filtering them against the caller's read access. Any authenticated user who knew another user's file id could have the builtin knowledge tools return indexed chunks from that file, causing a read-only cross-user confidentiality loss while leaving knowledge-base permissions and saved workspace model validation unaffected. This issue is fixed in 0.11.0.	2026-08-04	5.3	CVE-2026-70487
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.6.34 until 0.11.0, Open WebUI renders vega and vega-lite fenced code blocks in chat content by building a Vega view in the viewer browser without a restricted resource loader. Any user who can place such a block where another user will see it can make that user browser issue attacker-chosen outbound GET requests and read responses from same-origin or CORS-permissive targets into the rendered page. This issue is fixed in 0.11.0.	2026-08-04	4.1	CVE-2026-70480
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.7.0 until 0.11.0, the legacy chat-completions features block trusted a client-supplied image_generation flag and did not re-check the features.image_generation permission that the direct image routes and native function-calling path enforce. An authenticated user whose image-generation permission had been revoked could still consume the operator's configured image provider through chat completions, spending API credits and provider quota and writing generated files to operator storage, without exposing provider credentials or other users' data. This issue is fixed in 0.11.0.	2026-08-04	4.3	CVE-2026-70484
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 until 0.11.0, the sync cleanup endpoint authorized write access to the knowledge base in the URL but then acted on directory and file ids supplied in the request body without checking that those objects belonged to that knowledge base. A user with write access to one knowledge base could delete directories and remove file embeddings from another knowledge base, causing documents to drop out of retrieval results and breaking chat-with-file for targeted documents without disclosing contents. This issue is fixed in 0.11.0.	2026-08-04	4.3	CVE-2026-70488
openbao--openbao	OpenBao is an open source identity-based secrets management system. Prior to version 2.5.4, in OpenBao's Kerberos auth method on the 'GET' handler, or when an 'Authorization: Negotiate' header is supplied, the response is includes a 'logical.Auth' object in addition to an error message. This results in tokens being created with only the default policy, default TTL, and no entity information, which are hidden by the returned error message. No access to these tokens by the caller occurs and the authentication token is not ever made accessible outside of	2026-08-07	5.3	CVE-2026-46405

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`sys/raw`. This is fixed in OpenBao v2.5.4. As a workaround, users may set a rate limit quota to limit the creation of these paths. As the path is unauthenticated, it isn't possible to deny access to it.			
openemr--openemr	OpenEMR through 8.2.0 contains a stored cross-site scripting vulnerability in the patient portal template system that allows authenticated administrators to inject arbitrary HTML and JavaScript by storing malicious payloads through the template save mode, which only filters literal PHP open tags. Attackers can exploit the lack of output encoding at the template retrieval endpoint combined with missing HttpOnly cookie attributes to exfiltrate session tokens via document.cookie access, enabling full session hijacking of any admin, clinician, or portal patient who views a poisoned template.	2026-08-03	4.8	CVE-2026-67612
OpenHands--OpenHands	A vulnerability was determined in OpenHands up to 0.62.0. The affected element is the function initialize_repo of the file OpenHands/resolver/send_pull_request.py. This manipulation causes command injection. Remote exploitation of the attack is possible. The vendor deleted the original GitHub issue report. It appears that the affected path/file got removed in version 1.7.0.	2026-08-06	6.3	CVE-2026-19022
openshwprojects--OpenBK7231T_Ap p	OpenBK7231T's /cfg_wifi_set endpoint (src/httpserver/http_fns.c) accepts configuration changes via a plain GET request with no CSRF token. If the `web_admin_password_enabled` parameter is absent from the request, an else-branch silently clears the device's web admin password to an empty string. A one-click CSRF payload (e.g. an tag pointing at /cfg_wifi_set with new SSID/password parameters and web_admin_password_enabled omitted) visited by an authenticated admin's browser both hijacks the device's WiFi configuration and disables its web password protection.	2026-08-05	6.5	CVE-2026-71273
openshwprojects--OpenBK7231T_Ap p	OpenBK7231T's http_fn_ota_exec() (src/httpserver/http_fns.c) reflects the `host` query parameter directly into an HTML response via hprintf255(request, " OTA requested for %s! ", tmpA) with no HTML encoding, allowing a crafted URL such as /ota_exec?host=<script>alert(1)</script> to execute JavaScript in an authenticated admin's browser when they click a malicious link.	2026-08-05	5.4	CVE-2026-71275
OpenSIPS--opensips	OpenSIPS is a Session Initiation Protocol (SIP) server implementation. In versions prior to 3.6.6 and 4.0.0-rc1, the find_line_delimiter() function in the multipart body parser performs an out-of-bounds read via strncmp() when searching for MIME boundary delimiters. After finding a -- pattern near the end of the body, the function compares delimiter.len bytes (typically 20-70) starting from a position at or past the logical end of the body buffer, reading past the body boundary. The bug triggers when a SIP message has Content-Type: multipart/mixed with a boundary parameter and its body contains -- within two to three bytes of the body's end without being followed by the actual boundary delimiter. This issue has been fixed in versions 3.6.6 and 4.0.0-rc1.	2026-08-04	5.3	CVE-2026-45705
OpenStack--Ironic	In OpenStack Ironic through 38.0.0, a project reader that makes a crafted request to Ironic can return Portgroups assigned to Nodes owned or leased by another project.	2026-08-05	5	CVE-2026-71201
osCommerce--osCommerce	A security flaw has been discovered in osCommerce 4.14.63493. Affected by this issue is the function EmailController of the file app/lib/backend/controllers/EmailController.php of the component Email Template Configuration. Performing a manipulation of the argument email_templates_key results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	4.7	CVE-2026-18592
owen2345--camaleon-cms	Camaleon CMS through 2.9.2, fixed in commit 88ab703, contains a missing authorization vulnerability on the drafts endpoint that allows any authenticated low-privileged user to create draft posts by bypassing role and permission checks.	2026-08-03	4.3	CVE-2026-67616

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Attackers can send requests to the drafts endpoint using only session authentication to create unauthorized drafts that appear in the administrative drafts queue.			
paperless-ngx--paperless-ngx	Paperless-ngx's MailAccountViewSet.test() action, when called with an existing account's ID and a masked password field, reuses the stored password, account_type, refresh_token, and expiration from that existing account while allowing the caller to supply a different imap_server, imap_port, and imap_security in the same request. The test connection then authenticates to the caller-specified server using the real stored credentials. A user holding only object-level change_mailaccount permission on the target account (not full admin) can redirect the test connection to an attacker-controlled IMAP host, causing the real stored IMAP password or OAuth token to be sent to that host.	2026-08-05	6.5	CVE-2026-71244
perspective-dev--perspective	Perspective 5.0.0 contains a denial of service vulnerability that allows remote attackers to block the server event loop indefinitely by submitting a crafted expression containing unbounded for or while loop constructs in a TableMakeViewReq message. Attackers can embed an arbitrarily large iteration count in an expression column evaluated once per table row, causing the Tornado IOloop to block without any iteration cap, deadline, or cancellation check, rendering the server unresponsive to all connected clients.	2026-08-04	6.5	CVE-2026-67199
perspective-dev--perspective	Perspective 5.0.0 contains a cross-site scripting vulnerability in the built-in Debug plugin that allows attackers to inject arbitrary HTML and JavaScript by writing table cell values containing unescaped HTML markup, which are interpolated directly into innerHTML during CSV serialization rendering. Attackers can craft table rows with payloads such as unquoted attribute injections containing event handler attributes that bypass RFC 4180 quoting, since angle brackets and event handler attributes are never escaped before assignment, causing malicious scripts to execute in the embedding page's origin.	2026-08-04	5.4	CVE-2026-67196
PhialsBasement--KoboldCPP-MCP-Server	A weakness has been identified in PhialsBasement KoboldCPP-MCP-Server 1.0.0. Affected by this issue is the function makeRequest of the file src/index.ts of the component BaseConfigSchema. Executing a manipulation of the argument apiUrl can lead to server-side request forgery. It is possible to launch the attack on the local host. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	5.3	CVE-2026-19373
pilinux--gorest	GoRest is a Golang starter kit built with the Gin framework for prototyping and developing RESTful APIs. In versions prior to 1.12.2 nMemorySecret2FA contains a race condition due to an unsynchronized package-level map used to store 2FA secrets. Multiple HTTP handlers in handler/login.go and handler/twoFA.go read from and write to this map concurrently, and because Go's runtime treats unsynchronized concurrent map access as an unrecoverable fatal error, an attacker can repeatedly trigger this condition to crash the process on demand. This results in high, repeatable availability impact with no confidentiality or integrity consequences. This issue has been fixed in version 1.12.2.	2026-08-04	5.9	CVE-2026-48154
Pimzino--spec-workflow-mcp	A vulnerability was found in Pimzino spec-workflow-mcp up to 2.2.6. This issue affects the function ApprovalStorage.createApproval of the file src/tools/approvals.ts. Performing a manipulation of the argument categoryName results in path traversal. The attack is only possible with local access. Upgrading to version 2.2.7 is capable of addressing this issue. The patch is named 9c7a7839e690bb4543f0e7481b5740d23808e5fe. It is advisable to upgrade the affected component.	2026-08-09	5.3	CVE-2026-19336
pixelfed--pixelfed	Pixelfed's SearchController (behind the auth middleware) accepts a URL via its remote-search parameters and fetches it server-side through ActivityPubFetchService, whose validateUrl() only blocks the literal hosts 127.0.0.1, localhost, and ::1 and requires https, without checking the resolved IP against private, internal, or link-local ranges (e.g. 169.254.169.254). Optional DNS	2026-08-05	4.3	CVE-2026-71246

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validation is disabled by default and, when enabled, only confirms a DNS record exists without filtering by IP range. The fetch response body is returned to the requester only when the Content-Type matches an ActivityPub content type, making this a semi-blind but authenticated SSRF primitive reachable by any logged-in user.			
poco-ai--poco-agent	A security flaw has been discovered in poco-ai poco-agent up to 0.5.4. Affected is the function WorkspaceManager._setup_session_persistence of the file executor/app/core/workspace.py of the component Claude File Handler. The manipulation results in incomplete cleanup. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is told to be difficult. The exploit has been released to the public and may be used for attacks.	2026-08-06	4.8	CVE-2026-19019
Poesis--Rhymix CMS	A vulnerability was determined in Poesis Rhymix CMS up to 2.1.33. This impacts the function procImporterAdminCheckXmlFile of the file modules/importer/importer.admin.controller.php of the component Data Import Module. This manipulation of the argument filename causes server-side request forgery. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.1.34 will fix this issue. It is recommended to upgrade the affected component.	2026-08-05	4.7	CVE-2026-18856
ProjectSend--ProjectSend	ProjectSend r2029 contains a reflected cross-site scripting vulnerability in thumbnails-regenerate.php that allows remote attackers to inject arbitrary HTML and JavaScript by supplying unsanitized values in the start_date and end_date GET parameters, which are echoed unescaped into HTML attribute values. Attackers can craft a malicious URL that, when followed by an authenticated victim with edit_settings permissions, executes injected scripts in the application origin to steal session cookies or perform unauthorized actions including user management, file management, and application settings changes.	2026-08-05	6.1	CVE-2026-53992
properfraction--MailOptin	Contributor Cross Site Scripting (XSS) in MailOptin <= 1.2.78.0 versions.	2026-08-06	6.5	CVE-2026-66703
python-hyper--h2	h2 is a pure-Python implementation of a HTTP/2 protocol stack. Versions up to and including 4.4.0 accept request header blocks containing more than one Host header, and forward every Host header to the consuming application. Where the consumer downgrades HTTP/2 to HTTP/1.1, the resulting request carries two Host header lines, providing a request smuggling primitive. This issue is fixed in version 4.4.1.	2026-08-06	5.3	CVE-2026-71554
Qualcomm, Inc.--Snapdragon	Memory Corruption when processing registry values with incorrect types using a direct query method.	2026-08-04	6.7	CVE-2026-24076
Qualcomm, Inc.--Snapdragon	Information Disclosure when processing wireless network channel switch information with improperly formatted length fields.	2026-08-04	6.5	CVE-2026-24077
Qualcomm, Inc.--Snapdragon	Information Disclosure when IPSec negotiation fails or is not established properly during NG-eCall SIP signaling.	2026-08-04	6.5	CVE-2026-24078
RackTables--RackTables	A security vulnerability has been detected in RackTables up to 0.22.0/e5fff9f8aab339798ed47e8c6d7d977ed97a82bd. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The project maintainer confirms: "[I]t seems plausible, in that RackTables does not at this time have any CSRF prevention. You may assign a CVE ID to this, but there is no guarantee it will be handled in urgent, or even timely, manner, or at all."	2026-08-04	4.3	CVE-2026-18819
rclone--rclone	rclone is a command-line program to sync files and directories to and from different cloud storage providers. Prior to 1.75.0, a valid but nondefault FTP filename encoding in backend/ftp/ftp.go can restore raw CR/LF immediately before an attacker-controlled path is interpolated into the line-oriented FTP control	2026-08-05	6.4	CVE-2026-71311

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	channel, and github.com/jlaffaye/ftp formats the argument through textproto.Conn.Cmd without rejecting CR or LF, allowing a filename such as victim CRLF DELE other-secret CRLF NOOP to inject an independent authenticated FTP command when the victim copies or syncs to a more-privileged FTP destination. This issue is fixed in 1.75.0.			
rclone--rclone	rclone is a command-line program to sync files and directories to and from different cloud storage providers. From v1.51.0 until v1.75.0, the local backend in backend/local/local.go relies on the configurable filename encoder to prevent remote filename data from becoming operating-system path syntax, so a local destination using Slash, None, Raw, or on Windows an encoding that preserves backslash can decode a standard-encoded fullwidth dot-dot component or native backslash form into an actual parent-directory component before filepath.Join resolves it outside the configured local root, allowing an attacker-controlled source object to create or overwrite files outside the selected destination directory as the rclone process. This issue is fixed in v1.75.0.	2026-08-05	6.9	CVE-2026-71313
rclone--rclone	rclone is a command-line program to sync files and directories to and from different cloud storage providers. Prior to 1.75.0, the shared HTTP CONNECT helper in lib/proxy/http.go parses proxy CONNECT responses with http.ReadResponse over an unrestricted buffered reader, allowing a malicious or compromised configured proxy, or an active on-path actor controlling a plaintext HTTP proxy hop, to send oversized headers that grow memory until the rclone process fails. The affected helper is used by FTP and SFTP proxy connections, and SFTP reaches the parser before SSH server authentication, so target host key validation does not constrain a malicious proxy. This issue is fixed in 1.75.0.	2026-08-05	5.9	CVE-2026-71310
RealHomes Memberships--RealHomes Memberships	The RealHomes Memberships WordPress plugin before 3.1.0 does not verify that a membership payment actually completed, nor check a nonce or the user's capability, before granting a paid membership package, allowing any authenticated user such as a Subscriber to obtain paid membership packages without paying.	2026-08-06	4.3	CVE-2026-15246
Red Hat--Red Hat Build of Keycloak	A flaw was found in the SAML broker component of Keycloak, an identity and access management solution. When configured as a SAML broker using the IdP-Initiated flow, Keycloak fails to enforce the OneTimeUse condition in SAML assertions. This allows an attacker who captures a valid, unused assertion to replay it multiple times. Successful exploitation could allow an attacker to hijack a user's session and gain unauthorized access to the system as that user.	2026-08-06	6.4	CVE-2026-18967
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in the LDAP storage provider of Keycloak, which is used to federate user identities from external directories. The issue occurs when a delegated administrator performs a search using a specific LDAP entry Distinguished Name (DN). Due to missing validation, the system allows lookups for users located outside the configured search boundary, leading to the disclosure of account information from unauthorized parts of the directory and unintended importing of those users into local storage.	2026-08-05	5.4	CVE-2026-16071
Red Hat--Red Hat build of Keycloak 26.6	A flaw was found in the user-event metrics recording of Keycloak. When metrics are enabled, the system records raw error messages from failed account operations as Prometheus metric labels. Because these error messages can include user-supplied input like nonexistent client IDs, an authenticated user can create a massive number of unique metric entries, eventually exhausting system memory and causing the service to crash or become unavailable.	2026-08-05	6.5	CVE-2026-16100
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. During SASL PLAIN authentication, the server installs connection-level bind credentials before performing the account-lock check. If the account is subsequently found to be locked, the bind is reported as failed to the client, but the already-installed authenticated state on the connection is not reverted. A client that supplies valid credentials for an account that has been administratively locked can continue to use the same connection	2026-08-03	5.4	CVE-2026-18651

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with that account's privileges, defeating account lock as an access-revocation control.			
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in p11-kit. A local attacker, or one with equivalent access to a reachable RPC channel, could exploit an integer overflow vulnerability. By sending specially crafted messages, the attacker can cause the system to miscalculate memory allocation for nested attributes. This leads to a memory corruption issue, specifically a heap out-of-bounds write, which can crash the p11-kit RPC parsing process, resulting in a Denial of Service (DoS). This vulnerability is only exploitable on 32 bit systems.	2026-08-07	6.2	CVE-2026-18938
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in SSSD. The sss_nss_protocol_parse_addr() function in the NSS responder does not validate the addrlen field against the remaining packet body size. A local attacker can exploit this via a crafted GETHOSTBYADDR request to the NSS responder socket, causing an out-of-bounds read and process crash, resulting in a denial of service.	2026-08-03	5.5	CVE-2026-68742
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in SSSD. The extract_authtok_v1() function in the PAM responder does not validate the auth_token_length field against the remaining buffer size before processing. A local attacker can exploit this via a crafted protocol v1 request to the PAM responder socket, causing an out-of-bounds read and process crash, resulting in a denial of service.	2026-08-04	5.5	CVE-2026-68743
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in GIMP's file-png plugin. A remote attacker can exploit this by crafting a malicious Animated Portable Network Graphics (APNG) image containing an oversized tRNS chunk. This can lead to a stack-based buffer overflow (CWE-121), causing the file-png plugin to crash and resulting in a Denial of Service (DoS) for the user.	2026-08-03	5.5	CVE-2026-6694
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in GIMP. A remote attacker could exploit this by tricking a user into opening a specially crafted PAA (Paint Shop Pro Array) image file. This vulnerability, a heap-based out-of-bounds write in the decode_lzss() function of the PAA file format plugin, allows data to be written beyond the intended memory buffer. This could lead to heap metadata corruption and potentially enable the attacker to execute arbitrary code on the affected system.	2026-08-03	5.5	CVE-2026-6695
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in dhcp-server. A remote attacker with network access to the OMAPI (Open Management Application Programming Interface) port, especially if not secured with TSIG (Transaction Signature) key authentication, could send a specially crafted lease creation request. This request, containing an overly long InfiniBand MAC address, triggers a buffer overflow in the `print_hw_addr()` function. Successful exploitation leads to a persistent denial of service (DoS), causing the `dhcpd` service to crash and preventing it from restarting without manual intervention.	2026-08-04	4.9	CVE-2026-18103
Red Hat--Red Hat Hardened Images	A flaw was found in the RPM Package Manager (RPM). A local user could be affected by a heap buffer overflow vulnerability when processing a specially crafted NDB database file. This issue arises from an error in how RPM handles certain calculations during file parsing, leading to an incorrect memory allocation. An attacker could leverage this to cause a denial of service, making the system unavailable.	2026-08-05	5.5	CVE-2026-44605
Red Hat--Red Hat Hardened Images	A TOCTOU (Time-of-Check Time-of-Use) vulnerability in GNU tar's incremental dumpdir 'X' rename handling allows a local attacker with write access to a directory being backed up to influence the restore process if the attacker has access to the system where the restore is being performed. During restoration, files or directories may be created, renamed or overwritten outside the intended extraction directory. This could lead to unauthorized file modification or, in some cases, privilege escalation. Exploitation does not require the attacker to modify or craft the archive, and standard backup and restore workflows-including extracting	2026-08-03	4.4	CVE-2026-18477

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	into a newly created directory without using the -P option do not mitigate the issue.			
Red Hat--Red Hat Hardened Images	A flaw was found in GNU tar. When extracting an archive with the --one-top-level option, hardlink targets are not confined to the designated top-level directory and may resolve relative to the extraction working directory. A crafted archive can create hardlinks that escape the intended boundary and, when combined with a preexisting symbolic link under the working directory, may allow writing outside that boundary during a single extraction.	2026-08-03	4.4	CVE-2026-18508
Red Hat--Red Hat Hardened Images	A TOCTOU (Time-of-Check-Time-of-Use) race condition vulnerability was found in the fixfiles script in polycoreutils. When running fixfiles relabel or fixfiles restore, the script used find and chcon commands to locate and relabel unlabeled files under /tmp and other directories. A local attacker could exploit a race window between the file discovery and the label change operation by swapping directory components with symlinks, causing chcon to follow the symlink and modify SELinux labels on arbitrary system files. This could undermine SELinux mandatory access control protections on critical files such as /etc/shadow.	2026-08-07	4.4	CVE-2026-19079
Red Hat--Red Hat JBoss Enterprise Application Platform 7	A path traversal flaw was found in WildFly's domain mode implementation. The LocalFileRepository.getFile() and getConfigurationFile() methods in wildfly-core/deployment-repository do not validate that the resolved file path remains within the configured repository or configuration root directories. A remote attacker who has obtained the slave host controller secret or compromised a slave host controller can supply a crafted relative path containing directory traversal sequences (e.g., ../../etc/passwd) via the slave-DC wire protocol, causing the Domain Controller to resolve and serve arbitrary files readable by the DC process. This leads to unauthorized disclosure of sensitive information such as configuration files, keystores, and system credentials.	2026-08-04	4.4	CVE-2026-17614
Red Hat--Red Hat OpenShift Container Platform 4	A flaw was found in openshift/oauth-proxy. On paths configured to bypass authentication (skip-auth-regex), the proxy forwards client-supplied identity headers (X-Forwarded-User, X-Forwarded-Email, X-Forwarded-Access-Token) to the upstream application without stripping them. An unauthenticated attacker can inject forged identity headers on whitelisted paths.	2026-08-05	6.5	CVE-2026-49331
RegistrationMagic-RegistrationMagic	The RegistrationMagic WordPress plugin before 6.0.9.5 does not compare the verified PayPal capture's amount, currency, payee, or prior use against the registration it is finalising: its server-side check only confirms the capture status is COMPLETED. An unauthenticated attacker can therefore finalise an expensive paid registration with any genuinely-completed low-value capture, and replay a single capture across unlimited registrations because captures are not de-duplicated.	2026-08-06	5.3	CVE-2026-15208
Relevanssi--Relevanssi Premium A Better Search	The plugin provides an Admin Search page that allows users with the `edit_posts` capability to run Relevanssi searches from the WordPress dashboard. The AJAX handler accepts a URL-encoded `args` parameter, parses it into a `WP_Query`, and then passes user-controlled taxonomy query data into Relevanssi's taxonomy restriction builder. The taxonomy value is sanitized as text but is not parameterized for SQL before being interpolated into a term taxonomy lookup query. This allows an authenticated contributor-level attacker to inject SQL through the Admin Search AJAX request and execute time-based blind SQL injection against the WordPress database.	2026-08-05	6.5	CVE-2026-15941
Revenue Administration--E-Signature	Server-Side request forgery (SSRF) vulnerability in Revenue Administration Turkiye's E-Signature allows Server Side Request Forgery. This issue affects Turkiye's E-Signature: from 2.4.4.0 before 2.5.1.0.	2026-08-07	5.4	CVE-2026-16027
Saad Iqbal--Gutena Forms Contact Form, Survey Form, Feedback Form	Unauthenticated Broken Authentication in Gutena Forms - Contact Form, Survey Form, Feedback Form, Booking Form, and Custom Form Builder <= 1.9.0 versions.	2026-08-06	6.5	CVE-2026-66425

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Form, Booking Form, and Custom Form Builder				
Samsung Open Source--rlottie	Improper input validation vulnerability in Samsung Open Source rlottie allows Oversized Serialized Data Payloads.	2026-08-04	5.5	CVE-2026-18772
Scripta--eScriptorium	Authorization bypass in the process and annotation taxonomy serializers in Scripta eScriptorium through 26.04.1 allows a remote authenticated user to run segmentation and transcription against other users' document parts, overwriting their content, via part primary keys supplied to a many=True related field whose queryset restriction was applied to the ManyRelatedField instead of its child_relation and therefore had no effect	2026-08-06	6.5	CVE-2026-18275
Scripta--eScriptorium	Missing authorization in the websocket consumer in Scripta eScriptorium through 26.04.1 allows a remote authenticated user to subscribe to any document's event stream and observe another user's segmentation, transcription, import, export and training activity via the object_cls and object_pk values of a join-room message, which are passed to group_add without an access check	2026-08-06	4.3	CVE-2026-18276
SecureAge--CatchPulse	An improper access control check in CatchPulse's named pipe communication interface could allow an attacker to invoke CatchPulse functions. This is limited to operations that enforce more restrictive security policies.	2026-08-06	5.2	CVE-2026-55979
SecureAge--CatchPulse	A denial-of-service vulnerability in CatchPulse could allow an attacker to conduct a stack buffer overrun attack, leading to a denial-of-service condition.	2026-08-06	5.5	CVE-2026-55980
Security Optimizer--Security Optimizer	The Security Optimizer WordPress plugin from 1.5.8 to 1.6.4 does not correctly validate requests to its optional IP-based login restriction feature, allowing the restriction to be bypassed so that unauthenticated requests from non-allowlisted IP addresses can reach and use the login form, defeating the access control the administrator configured.	2026-08-06	5.3	CVE-2026-13342
seraphinitesoft--Seraphinite Accelerator	The Seraphinite Accelerator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'seraph_accel_prep' parameter in versions up to, and including, 2.29.15. This is due to the CacheExtractPreparePageParams() function using PHP's loose inequality operator (!=) to compare the expected HMAC string against the JSON-decoded 'nonce' value - supplying the JSON boolean true causes any non-empty HMAC string to compare as loosely equal, bypassing the signature check - combined with insufficient output escaping in the _CbContentFinishSkip() function, which concatenates the attacker-controlled 'selfTest' field directly into the HTML response body. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a specially crafted link.	2026-08-05	6.1	CVE-2026-17532
sevenspark--DTX Dynamic Text Extension for Contact Form 7	The Contact Form 7 - Dynamic Text Extension plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.0.5. This is due to insufficient output escaping on form shortcode keys displayed in the admin "Scan Forms for Post Meta and User Data Keys" page. This makes it possible for authenticated attackers, with Editor-level access and above, to inject arbitrary web scripts that execute when an Administrator runs the scan feature.	2026-08-05	4.4	CVE-2026-5116
shapedplugin--Easy Accordion AI-Powered FAQ & Accordion Blocks, Product FAQ	The Easy Accordion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'accordionTitleTag' block attribute in versions up to, and including, 3.1.8. This is due to insufficient input sanitization and output escaping in the accordion_header_renderer() function, which emits the attacker-supplied tag name using esc_attr() in an HTML tag-name context instead of tag_escape(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-08	6.4	CVE-2026-18988

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Sharp Corporation--Network Scanner Tool Lite	Network Scanner Tool and Network Scanner Tool Lite provided by Sharp Corporation, with the initial configuration, require no authentication and accept files unlimitedly. When the affected products are used with the initial configuration, anyone can connect to them without authentication and upload files unlimitedly. This may cause a denial-of-service (DoS) condition on the PC. Furthermore, if a malicious file is uploaded, a PC user may be tricked to execute the file to attack other entities from that PC.	2026-08-03	5.3	CVE-2026-62416
Sharp Corporation--Sharp MFPs	Sharp and Toshiba Tec MFPs (multifunction printers) for a certain market have been shipped with the user authentication feature disabled in the initial configuration. When used with the initial configuration, the address book editing and a range of features related to Document Filing can be accessed without user authentication. Products intended for the Japanese market are not affected.	2026-08-03	6.5	CVE-2026-63563
Sharp Corporation--Sharp MFPs	Sharp and Toshiba Tec MFPs (multifunction printers) fail to properly authorize requests to directly access certain image data stored to the affected product.	2026-08-03	5.3	CVE-2026-60011
shlinkio--Shlink	Shlink contains a blind SQL injection vulnerability that allows any authenticated API key holder to inject arbitrary SQL fragments by supplying an unvalidated direction value in the orderBy query parameter of the tag statistics endpoint. Attackers can craft a malicious direction string containing SQL subqueries that flows unsanitized into a Doctrine QueryBuilder ORDER BY clause, enabling time-based, boolean-oracle, and error-based extraction of sensitive data including long URLs, visitor records, IP addresses, geolocation data, user agents, and hashed API key secrets from any tenant.	2026-08-03	6.5	CVE-2026-18737
shlinkio--Shlink	Shlink contains a server-side request forgery vulnerability that allows authenticated API key holders to cause the server to issue arbitrary HTTP GET requests by supplying a crafted long URL during short URL creation with title auto-resolution enabled. Attackers can submit URLs pointing to public hosts that redirect to internal targets, including loopback addresses, link-local ranges, and cloud metadata endpoints such as 169.254.169.254, to exfiltrate internal service information via the HTML title element returned in the short URL creation response.	2026-08-03	5	CVE-2026-18736
shlinkio--Shlink	Shlink versions 5.0.0 through 5.1.5 contain a CSV formula injection vulnerability that allows unauthenticated remote attackers to plant spreadsheet formulas into exported visit data by supplying malicious values in User-Agent, Referer, or request path headers beginning with formula-triggering characters such as =, +, -, or @. Attackers can craft a single unauthenticated request against any short URL to embed DDE or WEBSERVICE formula payloads into CSV cells, which are then executed on an administrator's client machine when the exported CSV file is opened in a spreadsheet application that evaluates formulas.	2026-08-03	4.7	CVE-2026-18738
silverstripe--silverstripe-cms	Silverstripe CMS is an open source content management system. Prior to 6.2.1, page breadcrumbs in the CMS are vulnerable to cross-site scripting when viewed using the page list view, because page titles are rendered into the breadcrumb trail without being escaped. This issue is fixed in 6.2.1.	2026-08-06	5.4	CVE-2026-54717
Simple CAPTCHA with Cloudflare Turnstile--Simple CAPTCHA with Cloudflare Turnstile	The Simple CAPTCHA with Cloudflare Turnstile WordPress plugin before 1.42.0 does not bind its Turnstile validation cache to the single-use challenge token in its Forminator integration, instead keying it to an attacker-controlled, reusable request value, allowing unauthenticated attackers to solve one challenge and then replay token-less form submissions for a short window, defeating the anti-abuse protection the plugin provides.	2026-08-07	5.3	CVE-2026-15239
siyuan-note--siyuan	SiYuan versions before v3.7.3 contain a metadata disclosure vulnerability in the /api/block/getBlockInfo endpoint that returns document root metadata including title for publish-forbidden documents without publish-access checks. Anonymous readers or publish RoleReader tokens can supply a block ID to retrieve the title,	2026-08-03	5.8	CVE-2026-68585

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	notebook, path, root ID, and icon of documents administrators marked as excluded from publishing.			
smub--Smash Balloon Social Photo Feed Easy Social Feeds Plugin	The Smash Balloon Social Photo Feed - Easy Social Feeds Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via REQUEST_URI Query String in all versions up to, and including, 6.11.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2026-08-05	4.7	CVE-2026-15452
SNOMED International--Snowstorm	SNOMED International Snowstorm contains a reflected XSS vulnerability within the "Web Route" redirection functionality. An attacker can inject arbitrary JavaScript which will execute upon a target user navigating to a crafted, malicious link. Fixed in 10.12.2 and 10.9.3.	2026-08-04	5	CVE-2026-66300
sonalsinha21--SKT Skill Bar	The SKT Skill Bar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `chart_size` attribute of the `skillwrapper` shortcode in all versions up to, and including, 2.6. This is due to insufficient input sanitization and output escaping on the `chart_size` attribute, which is concatenated directly into an inline ` <style>` block. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.</td><td>2026-08-05</td><td>6.4</td><td>CVE-2026-6972</td></tr><tr><td>SourceCodester--Online Clothing Store</td><td>A vulnerability was determined in SourceCodester Online Clothing Store. Affected by this issue is some unknown functionality of the file /_notes/ of the component Dreamweaver Metadata Files. Executing a manipulation can lead to file and directory information exposure. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.</td><td>2026-08-07</td><td>5.3</td><td>CVE-2026-19229</td></tr><tr><td>SourceCodester--Online Examination & Learning Management System</td><td>A vulnerability was determined in SourceCodester Online Examination & Learning Management System 1.0. This issue affects some unknown processing of the file upload_files.php. This manipulation causes unrestricted upload. The attack may be initiated remotely.</td><td>2026-08-06</td><td>6.3</td><td>CVE-2026-19065</td></tr><tr><td>SourceCodester--Online Examination & Learning Management System</td><td>A vulnerability was found in SourceCodester Online Examination & Learning Management System 1.0. This vulnerability affects unknown code of the file /view.php. The manipulation of the argument ID results in authorization bypass. The attack can be launched remotely.</td><td>2026-08-06</td><td>4.3</td><td>CVE-2026-19064</td></tr><tr><td>SourceCodester--Online Examination & Learning Management System</td><td>A vulnerability was identified in SourceCodester Online Examination & Learning Management System 1.0. Impacted is an unknown function of the file view_students.php. Such manipulation of the argument class_group leads to authorization bypass. The attack may be launched remotely.</td><td>2026-08-06</td><td>4.3</td><td>CVE-2026-19066</td></tr><tr><td>SourceCodester--Photo Share Website</td><td>A vulnerability has been found in SourceCodester Photo Share Website 1.0. The impacted element is an unknown function of the file /social/ajax.php?action=save_upload. Such manipulation of the argument img[]/imgName[] leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.</td><td>2026-08-07</td><td>6.3</td><td>CVE-2026-19210</td></tr><tr><td>Spacebar Server--Spacebar Server</td><td>Spacebar Server before commit 51da17c contains a missing authorization vulnerability that allows any authenticated user to enumerate complete guild membership by querying the GET /guilds/{guild_id}/roles/{role_id}/member-ids endpoint without guild membership verification. Attackers can exploit the unprotected route handler in the roles member-ids endpoint, which lacks permission checks present in sibling endpoints, to retrieve the full list of member</td><td>2026-08-05</td><td>4.3</td><td>CVE-2026-70618</td></tr></table></style>			

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user IDs for any guild on the instance using only a valid bearer token and a known guild ID.			
spacetime--Ad Inserter Ad Manager & AdSense Ads	The Ad Inserter - Ad Manager & AdSense Ads plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.8.16 due to a missing capability check in the `ai_ajax` function. This makes it possible for unauthenticated attackers to view the contents of ad blocks that an administrator has restricted to administrator-only visibility.	2026-08-06	5.3	CVE-2026-11983
statamic--cms	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.74.1 and 6.24.0, an authenticated Control Panel user could view content from entries they did not have permission to view, including entry content and custom field values, from any collection and including unpublished entries, through the navigation endpoint, though no data could be modified. This issue is fixed in versions 5.74.1 and 6.24.0.	2026-08-06	6.5	CVE-2026-64662
statamic--cms	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.74.1 and 6.24.0, manipulating user-supplied input incorporated into Antlers templates could result in the loss of content and assets, on sites whose templates pass untrusted input into affected areas, and exploitation did not require authentication. This issue is fixed in versions 5.74.1 and 6.24.0.	2026-08-06	6.5	CVE-2026-64663
statamic--cms	Statamic CMS's user-augmentation resolver, AugmentedUser::get() in src/Auth/AugmentedUser.php, contains an explicit case for the `two_factor_recovery_codes` handle that returns the user's raw two-factor recovery codes with no access restriction: `if (\$handle === 'two_factor_recovery_codes') { return new Value(\$this->data->get('two_factor_recovery_codes'), ...); }`. Unlike sensitive fields such as password/password_hash, which are excluded from AugmentedUser entirely, two_factor_recovery_codes is neither excluded from augmentation nor present in Statamic's Antlers variable guard lists (guardedVariablePatterns/guardedContentVariablePatterns in src/Providers/ViewServiceProvider.php, and the runtime GlobalRuntimeState guard paths), which by default only guard config.app.key. On any Antlers template field where raw/dynamic template rendering is enabled for a given field (an admin/developer-configured, blueprint-level field option), a template such as `{{ current_user.two_factor_recovery_codes }}{{ value }}` renders the viewing user's own 2FA recovery codes directly into the HTML response, allowing an attacker who can view or capture that response (e.g. via a shared/observable page, or a crafted link causing a victim to render it) to obtain the codes and bypass 2FA. Exploitation requires that dynamic Antlers rendering already be enabled on a field the target user's data flows through, which is a blueprint-configuration privilege rather than a standard content-editing permission.	2026-08-05	6.2	CVE-2026-71293
statamic--cms	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.74.3 and 6.24.2, the default ("automagic") form notification email rendered user-submitted values without escaping, allowing an unauthenticated form submitter to inject HTML into the notification emails sent to the configured recipients. This issue is fixed in versions 5.74.3 and 6.24.2.	2026-08-06	6.1	CVE-2026-71435
statamic--cms	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.74.3 and 6.24.2, public frontend forms did not enforce the file upload restrictions that the Control Panel enforces, so an unauthenticated visitor could upload file types an administrator had intended to disallow through a form's assets or files field, and for assets fields, files could be stored on a public, web-accessible disk, though the application's global upload allowlist still blocked executable types such as .php and .html. This issue is fixed in versions 5.74.3 and 6.24.2.	2026-08-06	5.3	CVE-2026-71434
statamic--cms	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.74.1 and 6.24.0, an authenticated Control Panel user could use an endpoint	2026-08-06	4.3	CVE-2026-64664

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	intended for the user creation wizard to determine if a given email address belonged to an existing user, without having permission to view users, though the endpoint only exposed user existence and not any other user data. This issue is fixed in versions 5.74.1 and 6.24.0.			
Stephan Muelle--libkcapi	A flaw was found in libkcapi. When performing one-shot symmetric cipher operations on large inputs (over 64 KiB) in stateful modes such as Counter (CTR) or Cipher Block Chaining (CBC), the library improperly reuses the Initialization Vector (IV) for each internal data chunk. A remote attacker could potentially exploit this by making an application that uses libkcapi process specially crafted large inputs. This can lead to a significant weakening of data confidentiality, as the repeated IV use can expose relationships in encrypted plaintext, and may also affect data integrity by causing incorrect cryptographic processing.	2026-08-05	6.5	CVE-2026-71225
Stephan Muelle--libkcapi	A flaw was found in libkcapi. A local attacker can influence an application that uses the Asynchronous Input/Output (AIO) interface. By reusing an AIO-enabled handle after a prior completion error, the <code>_kcapi_aio_read_all()</code> function can enter a non-terminating wait loop. This can lead to a persistent denial of service, making the affected application or thread unresponsive.	2026-08-05	5.1	CVE-2026-71227
stiofansisland--UsersWP Front-end login form, User Registration, User Profile & Members Directory plugin for WP	The UsersWP - Front-end login form, User Registration, User Profile & Members Directory plugin for WP plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Badge Widget Variable Substitution in all versions up to, and including, 1.2.69 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-06	6.4	CVE-2026-18501
Strategy11 Team--Business Directory	Subscriber Cross Site Scripting (XSS) in Business Directory <= 6.4.24 versions.	2026-08-06	6.5	CVE-2026-61959
stylemix--Cost Calculator Builder	The Cost Calculator Builder plugin for WordPress is vulnerable to unauthorized access of sensitive data due to a missing capability check on the <code>'cost-calculator-custom-export-run'</code> AJAX action (handler <code>'CCBExportImport::export_calculators()'</code>) in all versions up to, and including, 3.6.17. The handler only verifies a nonce, but the corresponding <code>'ccb_export_nonce'</code> is broadcast on every wp-admin page (including pages reachable to Subscribers, such as <code>'/wp-admin/profile.php'</code>) by the <code>'ccb_add_admin_nonces'</code> callback hooked to <code>'admin_head'</code> . This makes it possible for authenticated attackers, with Subscriber-level access and above, to export every calculator's full configuration - including stored Stripe secret keys, PayPal client secrets, Razorpay secret keys, webhook secret keys, and reCAPTCHA secret keys.	2026-08-05	6.5	CVE-2026-7753
Subscriptions for WooCommerce--Subscriptions for WooCommerce	The Subscriptions for WooCommerce WordPress plugin before 2.0.1 does not validate the payment amount or bind the PayPal order token to the order being completed on the WooCommerce order-received flow: it captures a client-supplied token and marks the order paid whenever the capture status is COMPLETED, without comparing the captured amount to the order total. This allows an attacker (unauthenticated where guest checkout is enabled) to substitute an approved, uncaptured PayPal order token and have an expensive order marked paid without paying its price.	2026-08-07	5.9	CVE-2026-15211
supercleanse--PrettyLinks Affiliate Link Management, URL Shortener, Link Cloaking, Tracking & Branded Short Links	The PrettyLinks - Affiliate Links, Link Branding, Link Tracking, Marketing and Stripe Payments Plugin plugin for WordPress is vulnerable to SQL Injection via the 's' (search) parameter on the Pretty Links listing page in all versions up to, and including, 3.6.20. This is due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query in the <code>'search_links_table()'</code> function. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into	2026-08-05	4.9	CVE-2026-5062

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	already existing queries that can be used to extract sensitive information from the database.			
superpwa--Super Progressive Web Apps	The Super Progressive Web Apps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `superpwa_settings[offline_message_txt]` setting in all versions up to, and including, 2.2.43. This is due to insufficient input sanitization and output escaping. The offline message value is stored without sanitization, passed to the frontend via `wp_localize_script()` without escaping, and rendered using `innerHTML` in the JavaScript snackbar component. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user triggers the offline snackbar.	2026-08-05	4.4	CVE-2026-5108
SuperTokens Inc.--SuperTokens Core	A lack of tenant separation in SuperTokens Inc. SuperTokens Core v6.0.0 to v11.4.0 allows an authenticated party in one tenant to access sessions, data, and endpoints of another tenant.	2026-08-07	5.9	CVE-2026-37171
SureCart--SureCart	Unauthenticated Broken Access Control in SureCart <= 4.6.2 versions.	2026-08-06	5.3	CVE-2026-32548
SUSE--Rancher	The endpoint `/v3/import/{token}_{clusterId}.yaml` retrieves the cluster object before validating the token. When a valid cluster ID references a cluster that has private registry secrets configured, a nil pointer dereference in `pkg/systemtemplate/private_registry.go` causes the request to return HTTP 502 Bad Gateway. For cluster IDs that do not exist, the endpoint returns HTTP 200. This observable difference in response codes constitutes a reliable enumeration oracle.	2026-08-05	5.3	CVE-2026-55998
SUSE--Rancher	A denial-of-service vulnerability was identified in multiple TLS listeners in Rancher. Both the cattle-cluster-agent component running in downstream clusters and the Rancher server itself use the dynamiclistener library to serve TLS traffic. Without an effective CN filter configured, dynamiclistener automatically appended to each serving certificate any hostname presented via Server Name Indication (SNI) in incoming TLS requests. An unauthenticated attacker with network access within the affected cluster could send a large number of TLS requests with distinct hostnames, causing the serving certificate to accumulate an unbounded number of Subject Alternative Names (SANs). Eventually, the certificate grows large enough that TLS handshakes fail with an excessive message size error, causing a denial of service on the affected listeners.	2026-08-05	4.3	CVE-2026-55996
sveltejs--kit	SvelteKit is a framework for rapidly developing robust, performant web applications using Svelte. Prior to 2.70.2, the content negotiation header parser used by SvelteKit's request handling (for headers such as Accept) uses a regular expression vulnerable to quadratic backtracking, so a maliciously crafted header value can cause excessive CPU consumption and degrade or deny service. Version 2.70.2 fixes the issue.	2026-08-07	5.3	CVE-2026-66062
TBTAK BLGEM Software Technologies Research Institute--eta-otp-lock	Invocation of process using visible sensitive information vulnerability in TÄfÄ“BÄ,,Ä°TAK BÄ,,Ä°LGEM Software Technologies Research Institute eta-otp-lock allows System Footprinting. This issue affects eta-otp-lock: before 1.0.4.	2026-08-06	5	CVE-2026-18915
techeshita--Layouts for WPBakery	The Layouts for WPBakery plugin for WordPress is vulnerable to unauthorized actions due to a missing capability check on the `Layouts_WPB_Remote::template_sync()` callback registered via `wp_ajax_nopriv_handle_sync` in all versions up to, and including, 1.1.3. This makes it possible for unauthenticated attackers to force the WordPress server to issue outbound HTTP requests to the plugin vendor's external API (`https://www.layoutsforwpbakery.com/wp-json/layoutsforwpbakery/v1/{templates,categories}`) and to write the JSON-decoded responses verbatim into the site's `wp_options` table via `set_transient()`	2026-08-05	6.5	CVE-2026-7726

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	- at any rate the attacker chooses, with no nonce verification, capability check, or rate limiting.			
TestLinkOpenSourceTRMS--TestLink	TestLink 1.9.20 and prior contains an insecure direct object reference vulnerability that allows any authenticated user, including low-privilege guest accounts, to read arbitrary attachments by supplying an integer attachment ID to the attachmentdownload.php handler without any project or role authorization check. Attackers can enumerate sequential integer IDs through the attachment download endpoint to retrieve file contents from private projects they have no membership in, bypassing the per-project access control model and exposing test specifications, requirements documents, execution evidence, and other sensitive uploaded files across the entire installation.	2026-08-07	6.5	CVE-2026-70561
textPlus--Text Message and Call App	A vulnerability was identified in textPlus Text Message and Call App up to 8.3.5 on Android. This impacts the function DialerActivity of the component com.gogii.textplus. Such manipulation leads to improper export of android application components. The attack needs to be performed locally. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	2026-08-03	5.3	CVE-2026-18604
The-Pocket--PocketFlow (pocketflow-coding-agent cookbook example)	The pocketflow-coding-agent cookbook example in The-Pocket/PocketFlow implements a `_path(workdir, p)` helper as a thin os.path.join(workdir, p) wrapper with no canonicalization or containment check, used unguarded by the ReadFile, ListFiles, PatchRead, and PatchApply file-access tools. Because os.path.join returns an absolute `p` unchanged (ignoring workdir) and does not resolve `../` sequences, an agent invocation whose file-tool arguments include an absolute path or a traversal sequence can read or write files outside the configured working directory. Severity reflects that this affects an illustrative cookbook example rather than a core library API; applications that copy this pattern into production are affected.	2026-08-05	6.8	CVE-2026-55747
themefic--Ultra Addons for Contact Form 7	The Ultra Addons for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Range Slider 'data-label' and 'data-separator' attributes in all versions up to, and including, 3.5.43 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-07	6.4	CVE-2026-12801
themegrill--Accelerate	The Accelerate theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the enqueue_scripts() function in all versions up to, and including, 1.5.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install and activate the ThemeGrill Demo Importer plugin.	2026-08-06	4.3	CVE-2025-9266
thephpleague--commonmark	league/commonmark is a PHP library for parsing and rendering CommonMark Markdown. From 1.5.0 until 2.9.0, the AttributesExtension's href and src unsafe-link filter can be bypassed by embedding control bytes, such as a tab, carriage return, line feed, or leading C0 control character, in a javascript: URL that browsers discard before parsing the scheme, causing the browser to still execute the script even when the unsafe-link filter is enabled. This issue is fixed in 2.9.0.	2026-08-06	6.1	CVE-2026-71478
THM-Health--PILOS	PILOS (Platform for Interactive Live-Online Seminars) is a frontend for BigBlueButton. From 2.1.0 until 4.14.1, PILOS does not send a Cross-Origin-Opener-Policy response header, so pages opened by PILOS via a link that opens a new browsing context (e.g., target="_blank") retain a window.opener reference back to the originating PILOS tab. A malicious destination page reached this way can use window.opener to navigate or manipulate the original PILOS tab, a technique known as reverse tabnabbing, potentially redirecting an authenticated user to a phishing page that mimics PILOS. This issue is fixed in version 4.14.1.	2026-08-06	4.1	CVE-2026-71555
timescale--timescaledb	TimescaleDB through 2.29.1, fixed in commit 517c13e, contains an out-of-bounds read vulnerability in the Gorilla compression reverse row iterator that allows	2026-08-06	6.5	CVE-2026-70633

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attackers to cause a denial of service by storing a crafted compressed datum with an internally inconsistent BitArray. Attackers with DML access to a compressed hypertable can trigger an unsigned integer wraparound in the reverse iterator bucket index computation, causing a read beyond the end of the bucket array, resulting in a SIGSEGV crash that can be repeatedly triggered on each subsequent reverse-order scan.			
TinyAGI--TinyAGI	A vulnerability was detected in TinyAGI 0.0.20. The affected element is the function buildSystemPrompt of the file packages/server/src/routes/agents.ts. Performing a manipulation results in file inclusion. The attack may be initiated remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	5.3	CVE-2026-19011
trainingbusinesspros--Groundhogg CRM, Newsletters, and Marketing Automation	The Groundhogg - CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.5.2 via the GET /wp-json/gh/v4/contacts/<id> REST endpoint. The endpoint's permission callback checks only the role-level view_contacts capability and read_single() returns the full contact record by sequential integer ID without the object-level view_contact ownership check applied elsewhere in the codebase. This makes it possible for authenticated attackers holding view_contacts but not view_others_contacts - notably Groundhogg's built-in Sales Rep role, designed to see only its own contacts - to read any contact record on the site, including PII, contact meta, owner IDs, the admin edit URL, and (for contacts linked to a WordPress user) that user's full capability set.	2026-08-05	6.5	CVE-2026-11454
TryGhost--Ghost	Ghost is a Node.js content management system. From 0.10.0 until 6.54.1, a vulnerability in custom themes allowed a staff user to write files outside of the uploads directory. This could be used to alter the behavior of the installation through custom theme upload path traversal in LocalStorageBase and theme storage name handling. This issue is fixed in version 6.54.1.	2026-08-04	6.6	CVE-2026-70593
TryGhost--Ghost	Ghost is a Node.js content management system. From 2.2.0 until 6.54.1, Ghost Admin did not invalidate existing sessions on login which could have allowed for session fixation attacks. Successful exploitation would have required another vulnerability on the same domain where Ghost Admin was hosted. This issue is fixed in version 6.54.1.	2026-08-04	6.7	CVE-2026-70594
TryGhost--Ghost	Ghost is a Node.js content management system. From 5.26.0 until 6.54.1, the Universal Import feature in Ghost Admin failed to properly sanitize imported content resulting in XSS in post content. This issue is fixed in version 6.54.1.	2026-08-04	5	CVE-2026-70588
TryGhost--Ghost	Ghost is a Node.js content management system. From 1.20.1 until 6.54.1, an Administrator-level user could remotely overwrite certain files on the filesystem through the database backup filename, leading to integrity and availability issues. The database export endpoint failed to reject path separators in the caller-supplied filename. This issue is fixed in version 6.54.1.	2026-08-04	5.5	CVE-2026-70592
TryGhost--Ghost	Ghost is a Node.js content management system. From 4.22.0 until 6.54.1, a missing validation check allowed users to redeem subscription offers that were no longer active. This issue is fixed in version 6.54.1.	2026-08-04	4.8	CVE-2026-70589
TryGhost--Ghost	Ghost is a Node.js content management system. Prior to 6.54.1, any staff-level user was able to leak the hashed passwords of other staff users through the Ghost Admin API. An offline password-guessing attack against the hashes could lead to account takeover if successful, but Device Verification should have prevented an attacker from logging in with a recovered password. Depending on the database used, leaked hashes may not have had the correct casing for all characters, increasing the difficulty of a password-guessing attack. This issue is fixed in version 6.54.1.	2026-08-04	4.8	CVE-2026-70590
TryGhost--Ghost	Ghost is a Node.js content management system. From 0.10.0 until 6.54.1, a Server-Side Request Forgery in Ghost Admin image fetching allowed any staff-level user to	2026-08-04	4.1	CVE-2026-70591

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	perform a blind HTTP GET request against internal hosts. No output was returned, but this could have been used to probe open ports on internal hosts. This issue is fixed in version 6.54.1.			
TryGhost--Ghost	Ghost is a Node.js content management system. From 6.26.0 until 6.54.1, a validation issue allowed some functionality, such as Webmentions, to be abused by an unauthenticated user to make limited HTTP requests to hosts in the Ghost server's internal network. A successful attack would not result in any response data being returned. This vulnerability is fixed in 6.54.1.	2026-08-05	4	CVE-2026-70595
TryGhost--Ghost	Ghost is a Node.js content management system. From 4.9.0 until 6.54.1, an input validation issue allowed any staff user to create a post with content in feature_image_caption that could be used to hijack another staff user's Ghost Admin session, resulting in privilege escalation. This issue is fixed in 6.54.1.	2026-08-05	4.3	CVE-2026-70596
ttttonyhe--OBlog	A security vulnerability has been detected in ttttonyhe OBlog up to 3ca6a45a2fcc81f6086751d8af124658720e8f8f. This issue affects some unknown processing of the file /tags.php. Such manipulation of the argument day leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	4.3	CVE-2026-18968
Tutor LMS--Tutor LMS	The Tutor LMS WordPress plugin before 3.9.14 does not properly verify enrollment when restricting access to protected course content, allowing authenticated users with subscriber-level access and above who are enrolled in at least one course to view paid lesson, quiz, and assignment content belonging to other courses.	2026-08-06	4.3	CVE-2026-14306
uhop--node-re2	node-re2 provides RE2 regular expression bindings for Node.js. Prior to version 1.25.1, the WrappedRE2::Replace function built its replacement result and passed it to V8 using ToLocalChecked without checking for the empty MaybeLocal that V8 returns when the resulting string or buffer exceeds V8's maximum string length. When a global replace uses an output amplifying replacement template, the result can grow quadratically with the input size, and once the result exceeds V8's maximum string length, the unchecked ToLocalChecked call causes a fatal, uncatchable process abort instead of a catchable exception. This issue is fixed in version 1.25.1.	2026-08-06	6.2	CVE-2026-71430
uhop--node-re2	node-re2 provides RE2 regular expression bindings for Node.js. Prior to version 1.26.1, passing a Buffer whose final bytes form a truncated (incomplete) multi-byte UTF-8 sequence could cause the native binding to read past the end of the allocated buffer while attempting to decode the final, incomplete code point. This could result in an out-of-bounds read and potential disclosure of adjacent memory contents. This issue is fixed in version 1.26.1.	2026-08-06	5.1	CVE-2026-71498
Unlimited Elements--Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	Contributor Arbitrary File Download in Unlimited Elements For Elementor (Free Widgets, Addons, Templates) <= 2.0.14 versions.	2026-08-06	6.5	CVE-2026-28146
Unlimited Elements--Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	Missing Authorization vulnerability in Unlimited Elements Unlimited Elements For Elementor (Free Widgets, Addons, Templates) allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Unlimited Elements For Elementor (Free Widgets, Addons, Templates): from n/a through 2.0.15.	2026-08-03	5.4	CVE-2026-28147

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Vladimir Garagulya--Plugins Garbage Collector (Database Cleanup)	Unauthenticated Cross Site Request Forgery (CSRF) in Plugins Garbage Collector (Database Cleanup) <= 0.14 versions.	2026-08-06	6.5	CVE-2026-66686
vxcontrol--PentAGI	A weakness has been identified in vxcontrol PentAGI up to 2.1.0. This affects an unknown part of the file backend/pkg/templates/prompts/pentester.tmpl of the component Tool Management Protocol Handler. Executing a manipulation can lead to sandbox issue. It is possible to launch the attack remotely. The attack requires a high level of complexity. It is indicated that the exploitability is difficult. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	5.6	CVE-2026-18593
Wavlink--WL-NU516U1	A vulnerability was determined in Wavlink WL-NU516U1 708c073-mt7628. Affected is the function set_sys_adm of the file adm.cgi of the component Admin Password Handler. This manipulation causes os command injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. It is suggested to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-08-03	6.3	CVE-2026-18590
webcoders--Udimi Tools	The Udimi Tools plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `ajax_disconnect()` function in all versions up to, and including, 3.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete the plugin's six configuration options - including the API key, connected Udimi user email, and tracking-script payload - effectively disconnecting the site from the configured Udimi account. The companion `ajax_connect()` handler is missing the same checks, allowing the same low-privilege attackers to overwrite those options with an attacker-supplied API key.	2026-08-05	6.5	CVE-2026-7456
wedevs--ERP: Complete HR, Accounting & CRM Suite Built for WooCommerce	The ERP: Complete HR, Accounting & CRM Suite with WooCommerce CRM Support plugin for WordPress is vulnerable to SQL Injection via the 'erpadvancefilter' parameter in all versions up to, and including, 1.17.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. The handler runs the value through sanitize_text_field, which preserves single quotes, and the downstream erp_crm_contact_advance_filter() function interpolates it directly into a single-quoted SQL WHERE clause before execution via \$wpdb->get_results(). This makes it possible for authenticated attackers, with the plugin-supplied CRM Agent role (or higher CRM Manager / WordPress admin) and the erp_crm_list_contact capability, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-05	6.5	CVE-2026-11421
WonderTrader--WonderTrader	A weakness has been identified in WonderTrader up to 0.9.9. This vulnerability affects the function MatchEngine::update_job of the file src/WtBtCore/MatchEngine.cpp of the component Internal Limit Order Book Cache Handler. This manipulation causes enforcement of behavioral workflow. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	4.3	CVE-2026-19037
WonderTrader--WonderTrader	A vulnerability was determined in WonderTrader up to 0.9.9. This impacts an unknown function of the file src/Includes/WTSTradeDef.hpp of the component TraderATP Cash Trade Conversion. Executing a manipulation of the argument m_offsetType can lead to use of uninitialized variable. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-07	4.3	CVE-2026-19212

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WonderTrader--WonderTrader	A vulnerability was identified in WonderTrader up to 0.9.9. Affected is the function <code>_undone_qty</code> in the library <code>src/WtCore/TraderAdapter.h</code> of the component Pending Order Handler. The manipulation of the argument <code>getUndoneQty</code> leads to enforcement of behavioral workflow. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-07	4.3	CVE-2026-19213
wongcyrus--ExcelLexBot	A vulnerability was detected in wongcyrus ExcelLexBot up to 0.0.3. This affects the function <code>ExcelLexBotS3TriggerFunction</code> of the component Lambda Function Handler. Performing a manipulation results in improper privilege management. The attack may be initiated remotely. The vendor was contacted early about this disclosure but did not respond in any way. This vulnerability only affects products that are no longer supported by the maintainer.	2026-08-09	4.7	CVE-2026-19360
WP Events Manager--WP Events Manager	The WP Events Manager WordPress plugin before 2.2.5 does not verify that an incoming payment notification originates from the site's configured merchant account, nor that the paid amount matches the booking total, allowing unauthenticated users to mark any booking as paid without a legitimate payment reaching the merchant, including other users' bookings.	2026-08-07	5.3	CVE-2026-15148
WP Hotel Booking--WP Hotel Booking	The WP Hotel Booking WordPress plugin before 2.3.3 does not ensure that room quantities and the resulting order total are non-negative when placing a booking, and relies on client-controlled cart data, allowing unauthenticated users to create confirmed reservations for free or at an arbitrarily reduced price.	2026-08-06	5.3	CVE-2026-15149
WP Hotel Booking--WP Hotel Booking	The WP Hotel Booking WordPress plugin before 2.3.2 does not verify that a payment notification corresponds to a payment made to the site's own merchant account, nor that the paid amount matches the booking total, allowing unauthenticated users to have their bookings marked as fully paid without any payment reaching the site owner.	2026-08-06	5.3	CVE-2026-15152
WP Travel Engine--WP Travel Engine	The WP Travel Engine WordPress plugin before 6.8.2 does not verify that an incoming PayPal payment notification was sent to the site's configured merchant account, nor that the paid amount matches the order total, before marking a booking as paid, allowing unauthenticated attackers to mark bookings as fully paid using a token payment made to an attacker-controlled account.	2026-08-06	5.3	CVE-2026-12501
WP Zone--Custom CSS and JavaScript	Unauthenticated Sensitive Data Exposure in Custom CSS and JavaScript <= 2.0.16 versions.	2026-08-06	5.3	CVE-2026-66683
WPKube--CAPTCHA 4WP	Unauthenticated Bypass Vulnerability in CAPTCHA 4WP <= 7.6.0 versions.	2026-08-06	5.3	CVE-2026-32469
wpxpo--Post Grid Gutenberg Blocks PostX	The Post Grid Gutenberg Blocks for News, Magazines, Blog Websites - PostX plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the <code>'inputPlaceHolder'</code> parameter in all versions up to, and including, 5.0.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-06	6.4	CVE-2026-5158
WSO2--WSO2 API Control Plane	The user self-signup flow in multiple WSO2 products fails to adequately validate user-supplied input. This weakness allows arbitrary unvalidated data to be included within user claims, which are then used by downstream processes. Allowing unvalidated input into user claims can lead to various security risks. Malicious or malformed data injected during signup could be processed by other parts of the application, potentially enabling attacks such as content manipulation, redirection, user interface inconsistencies, unauthorized actions, and data exposure. The actual impact depends on how the compromised data is consumed and the privileges associated with the affected users.	2026-08-06	4	CVE-2024-10302

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WSO2--WSO2 API Manager	Unused authorization codes issued to deleted users are not being properly invalidated or removed from the system. This allows for the persistence of these codes, enabling them to be potentially reused. If an attacker possesses both the authorization code and the associated client credentials (client ID and client secret), they can leverage these unused codes to obtain access tokens on behalf of users who have already been deleted. This may lead to unauthorized access to sensitive resources and services, contingent on the scopes originally authorized for the compromised authorization code.	2026-08-06	4.9	CVE-2024-8995
WSO2--WSO2 API Manager	The Swagger UI Try-out console within the API Publisher documentation allows an external Swagger API definition URL to be loaded, overriding the existing API definitions within the Publisher portal. By exploiting this vulnerability, malicious actors can deceive users into interacting with these overwritten API definitions. This could lead to the exposure of sensitive information or the initiation of unintended requests to backend services.	2026-08-06	4.3	CVE-2025-6508
WSO2--WSO2 API Manager	When an Event Publisher output adapter is configured with irrelevant properties, the affected products log these properties. This logging occurs without sufficient validation or sanitization of the property values. A malicious actor with access to the 'wso2carbon' log files could retrieve sensitive information, such as user credentials or other confidential data, that was inadvertently logged due to misconfiguration, potentially leading to unauthorized access.	2026-08-06	4.4	CVE-2026-0637
WSO2--WSO2 Enterprise Integrator	The account locking mechanism fails to trigger when secondary user stores are inaccessible. The software does not maintain a consistent state for account locking if it cannot reach all configured user stores, allowing an attacker to repeatedly attempt authentication with invalid credentials without triggering the lockout mechanism for users within active stores. When the account locking mechanism is bypassed due to the inaccessibility of secondary user stores, users in accessible user stores are left vulnerable to brute force attacks. A malicious actor can exploit this by attempting numerous invalid password combinations against a user account without the expected account lockout consequence.	2026-08-06	5.9	CVE-2024-6832
WSO2--WSO2 Enterprise Integrator	When internal roles are removed from a user within the WSO2 product, the system fails to invalidate any previously issued authentication tokens associated with that user. This vulnerability could allow users to retain their previous access privileges even after their roles have been revoked. As a result, a user can continue to perform unauthorized actions or access restricted resources until the expired tokens naturally expire.	2026-08-06	5	CVE-2025-12317
WSO2--WSO2 Identity Server	The Ajax processor within the Carbon console fails to adequately protect state-changing operations from Cross-Site Request Forgery (CSRF) attacks. Specifically, it utilizes the HTTP GET method for these operations, and while the SameSite=Lax cookie attribute is employed for mitigation, this mechanism is bypassed as it permits cookies to be sent with cross-origin top-level navigation requests, including GET requests. This allows an attacker to trick an authenticated user's browser into unknowingly executing unintended actions. An attacker can exploit this vulnerability to perform unauthorized state-altering requests on behalf of authenticated users. This could lead to consequences such as data modification, account changes, or other actions that could result in data compromise or loss of user control over their account. However, this attack is only feasible if the Carbon console and related services are exposed to the public internet, which is not recommended according to WSO2's security guidelines.	2026-08-06	5.4	CVE-2025-13394
WSO2--WSO2 Identity Server	When secondary user stores are configured, the implicit-association resolver incorrectly initializes from a secondary user store and bypasses the primary user store during search and uniqueness checks. This allows a subject to be associated with an unintended local account if the same lookup claim (e.g., username or email) exists in both the primary and a secondary store. If duplicate claim values exist across user stores, this issue can lead to identity confusion due to incorrect implicit associations when using an external Identity Provider (IDP). Legitimate user	2026-08-06	4.3	CVE-2025-11850

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accounts in the primary user store may fail to associate correctly with their corresponding external IDP accounts, potentially restricting access if the secondary account has fewer privileges. Deployments are not affected if no secondary user stores are configured, implicit association is disabled, or claim values are globally unique.			
WSO2--WSO2 Identity Server	The system accepts authentication requests without sufficient validation to enforce tenant isolation when using Email OTP, SMS OTP, or Magic Link as first-factor authenticators. This failure to adequately separate user data between tenants can lead to the exposure of personally identifiable information. Successful exploitation allows an attacker to disclose personally identifiable information of users in different tenants, resulting in privacy violations and potential regulatory non-compliance. This may include unauthorized access to user details such as mobile numbers.	2026-08-06	4.3	CVE-2025-13909
WSO2--WSO2 Micro Integrator	The Class Mediator fails to correctly validate or sanitize `messageContext` properties when they are used to populate dynamic values. This allows authenticated users to potentially access or modify data across different system invocations that should be isolated. This weakness can lead to the disclosure of sensitive information belonging to other users or the unintended modification of system data by authenticated users. The exact impact depends on how `messageContext` properties are utilized within the affected WSO2 products.	2026-08-06	6.8	CVE-2024-6541
xpro--Xpro Addons 140+ Widgets for Elementor	The Xpro Addons plugin for WordPress is vulnerable to unauthorized creation of data due to a missing capability check on the `get_menu_content_editor()` function in all versions up to, and including, 1.5.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create arbitrary published posts of the `xpro_content` custom post type with attacker-controlled titles. The created posts are publicly queryable on the front-end, enabling content injection, SEO spam, and database pollution.	2026-08-05	4.3	CVE-2026-7105
xwp--Stream Activity Log & Audit Trail	The Stream plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.2.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to access all Stream activity records via the Heartbeat API.	2026-08-07	6.5	CVE-2026-11907
yeqifu--warehouse	A vulnerability was determined in yeqifu warehouse up to aaf29962ba407d22d991781de28796ee7b4670e4. This issue affects some unknown processing of the file src/main/java/com/yeqifu/sys/controller/FileController.java. This manipulation of the argument path causes path traversal. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. This product is using a rolling release to provide continuous delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	4.3	CVE-2026-18903
YITHemes--YITH WooCommerce Zoom Magnifier	Unauthenticated Sensitive Data Exposure in YITH WooCommerce Zoom Magnifier <= 2.52.0 versions.	2026-08-06	5.3	CVE-2026-28169
yushine--InnoShop	A flaw has been found in yushine InnoShop up to 0.8.2. Affected by this issue is the function FileManagerController::destroyFiles of the file innopacks/restapi/routes/panel-api.php of the component Files Endpoint. This manipulation causes path traversal. The attack may be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-05	5.4	CVE-2026-18959
zephyrproject--zephyr	The SF32LB MPI QSPI NOR flash driver (drivers/flash/flash_sf32lb_mpi_qspi_nor.c) validated the flash offset and length on its read and write paths with the test (offset + size) > data->size. Because offset is a signed off_t while size is unsigned, a negative offset is converted to a large unsigned value and the addition can wrap to	2026-08-07	6.6	CVE-2026-11743

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a small result that passes the check. The read path then performs memcpy(dst, (void *) (data->base + offset), size) and the write path programs flash at offset and cache-invalidates data->base + offset, in both cases accessing memory outside the mapped flash window. The driver's erase path already rejected negative offsets, but read and write did not. In builds with CONFIG_USERSPACE, flash_read and flash_write are syscalls whose verifiers validate the device object and the caller's buffer but deliberately delegate offset bounds checking to the driver. An unprivileged thread that has been granted access to this flash device can therefore call the syscall with a crafted negative offset and a buffer valid in its own memory domain, and reach the unchecked access. The most direct impact is on the read path: by choosing a negative offset and matching size, an attacker slides the memcpy source below the flash base and copies arbitrary CPU-addressable memory into its own buffer, disclosing memory it is not authorized to read. The write path additionally allows programming flash at an out-of-range address and invalidating an attacker-chosen cache range, affecting integrity and availability. Reachability requires userspace to be enabled and the raw flash device object to be granted to an untrusted thread. The fix replaces the check with qspi_nor_range_is_valid(), which rejects negative offsets and performs the bound comparison in overflow-safe 64-bit arithmetic on both paths, and additionally adds an SRAM DMA bounce buffer plus source/destination overlap rejection to prevent a separate DMA bus-hang condition.			
zhayujie--CowAgent	A vulnerability was detected in zhayujie CowAgent up to 2.1.1. This vulnerability affects the function _select_tools of the file agent/evolution/executor.py of the component Self-Evolution Review Agent. Performing a manipulation results in incorrect authorization. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2026-08-06	6.3	CVE-2026-18992
Zombodroid--Meme Generator App	A security vulnerability has been detected in Zombodroid Meme Generator App 4.6830 on Android. This issue affects the function t5.l.c of the component com.zombodroid.MemeGenerator. Such manipulation leads to path traversal. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	5.3	CVE-2026-18853
ZTE--F689	By accessing unencrypted information in the device firmware, an attacker can obtain credentials related to the integrity verification of a specific application function on the device.	2026-08-07	6.5	CVE-2026-49008
ZTE--F689	By accessing unencrypted information in the device firmware, an attacker can obtain credentials related to TLS transmission.	2026-08-07	5.3	CVE-2026-49006
ZTE--NX799J (Red Magic 11 Air)	The built-in PostgreSQL service on the mobile device suffers from misconfiguration flaws and command injection vulnerabilities. This service listens on a specific port, runs with root privileges, and is protected by weak credentials. The database supports the COPY FROM PROGRAM syntax, allowing local attackers to bypass Android's permission sandbox and gain full root access.	2026-08-05	6.5	CVE-2026-49004
Zyxel--WAX650S firmware	An improper authentication vulnerability in the "social_login.cgi" CGI program in Zyxel WAX650S firmware versions through 7.10(ABRM.4)C0 could allow an attacker on the WLAN to bypass captive portal authentication.	2026-08-04	6.5	CVE-2026-8508
10web--Form Maker by 10Web Mobile-Friendly Drag & Drop Contact Form Builder	The Form Maker by 10Web - Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to blind SQL Injection via '{username}' Placeholder in Dynamic-Choice Field WHERE Clause in all versions up to, and including, 1.15.44 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This requires that a form is configured with a DB-backed dynamic choice field whose WHERE template references the	2026-08-15	5.3	CVE-2026-15993

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	{username} placeholder, and the attacker must first set their own display_name to a SQL payload via the standard WordPress profile edit screen before triggering the fm_reload_input AJAX endpoint.			
648540858--wvp-GB28181-pro	A vulnerability was identified in 648540858 wvp-GB28181-pro 2.7.4-20260107. This affects an unknown part of the file PlayController.java of the component Snapshot Endpoint. The manipulation of the argument deviceId/channelId leads to path traversal. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-08-14	6.3	CVE-2026-19828
648540858--wvp-GB28181-pro	A security flaw has been discovered in 648540858 wvp-GB28181-pro 2.7.4-20260107. This vulnerability affects unknown code of the file LogController.java of the component Log File Download Endpoint. The manipulation of the argument fileName results in path traversal. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-08-14	4.3	CVE-2026-19829
@fastify/oauth2--@fastify/oauth2	@fastify/oauth2 is an OAuth 2.0 plugin for Fastify. In versions from 7.2.0 up to but not including 8.3.0, the plugin validates the OAuth state, and with PKCE the code verifier, by comparing the callback query parameter against an unprefixed, predictable cookie, with no server-side binding to the browser that began the flow. Any party able to write a cookie for the application's host, such as a sibling subdomain under the same registrable domain, can plant matching state and verifier cookies and complete an attacker-owned OAuth flow inside a victim's browser, silently signing the victim in to the attacker's account (login CSRF). It does not expose the victim's own account, credentials, or tokens. The issue is fixed in @fastify/oauth2 8.3.0, which adds an opt-in hostPrefixedCookies option. Users should upgrade to 8.3.0 and enable it, or bind state to a server-side session.	2026-08-15	4.2	CVE-2026-18165
activepieces--activepieces	Activepieces is an open source AI workflow automation platform. Prior to 0.83.0, the /api/redirect OAuth callback endpoint embeds the user-supplied code query parameter directly into an inline script block without proper escaping. A crafted request to /api/redirect with a malicious code value can break out of the script context and execute arbitrary JavaScript in the Activepieces origin when a logged-in user opens it. An unauthenticated attacker can access the victim's session tokens or make authenticated API calls on the victim's behalf. This issue is fixed in version 0.83.0.	2026-08-11	6.1	CVE-2026-73084
AcyMailing Newsletter Team--AcyMailing SMTP Newsletter	Subscriber Broken Access Control in AcyMailing SMTP Newsletter <= 10.11.1 versions.	2026-08-13	6.5	CVE-2026-28181
AcyMailing Newsletter Team--AcyMailing SMTP Newsletter	Subscriber Cross Site Scripting (XSS) in AcyMailing SMTP Newsletter <= 10.11.1 versions.	2026-08-13	6.5	CVE-2026-28182
AcyMailing Newsletter Team--Anti Spam and list cleaner AcyChecker	Unauthenticated Broken Access Control in Anti Spam and list cleaner – AcyChecker <= 2.0.0 versions.	2026-08-13	6.3	CVE-2026-66689
Admidio--admidio	Admidio is an open-source user management solution. Prior to version 5.0.10, an authenticated Admidio member with upload rights on any one folder can permanently delete files from folders where they have only view access. The authorization check at the top of `modules/documents-files.php` evaluates upload rights against the attacker-supplied `folder_uuid` URL parameter - not the file's actual parent folder. The `file_delete` handler then only verifies view rights on the file's real location, never upload rights. By passing a folder they legitimately own in `folder_uuid` while targeting a file in a restricted folder via `file_uuid`, an attacker	2026-08-12	6.5	CVE-2026-47226

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bypasses the upload-right check entirely and permanently deletes the file. This is an incomplete fix of GHSA-rmpj-3x5m-9m5f, which was patched in v5.0.7 but remains exploitable in v5.0.9. User should upgrade to v5.0.10 to receive an updated fix.			
Admidio--admidio	Admidio is an open-source user management solution. `modules/categories.php` checks that the supplied `type` parameter (`ANN`, `EVT`, `ROL`, `USF`, `I`) corresponds to a module the actor administers. The follow-up "is this specific category editable by me" check at lines 56-61 is dead code because it compares `\$getType` (a category-type code) against mode names (`edit`/`save`/`delete`); the condition is permanently false, so `\$category->isEditable()` is never invoked. Prior to version 5.0.10, the `delete`, `sequence`, and `save` switch cases load the category by the supplied UUID and act on it without re-checking that the category belongs to a module the actor administers. A user holding only one module-administrator right can therefore destroy or reorder empty categories belonging to *other* modules - for example, an announcements administrator can delete role categories, profile-field categories, or weblink categories that they have no right to touch. Version 5.0.10 fixes the issue.	2026-08-12	6.5	CVE-2026-47227
Admidio--admidio	Admidio is an open-source user management solution. Prior to version 5.0.10, `modules/documents-files.php` mode `file_rename_save` shares the same root-cause shape as the cross-folder move bug (`05-documents-cross-folder-move-idor.md`): the top-level rights check at lines 79-89 validates `hasUploadRight()` on the URL parameter `folder_uuid`, but the rename operation acts on `file_uuid` - a separate URL parameter - without re-checking the folder that actually contains the file. `DocumentsService::renameFile()` resolves the target file via `getFileForDownload()` (which permits view-readable files) but does not require upload right on the file's source folder. Result: a user with upload right on any folder A can rename a file in folder B as long as they can view it. They can also overwrite the file's description. Version 5.0.10 contains a fix.	2026-08-12	6.5	CVE-2026-47230
Admidio--admidio	Admidio is an open-source user management solution. Version 5.0.9 added a missing `isAdministratorInventory()` gate to `case 'item_delete':` in `modules/inventory.php`. The same fix was not applied to the sibling `case 'field_delete':` handler, which destroys an entire inventory field definition, cascading to every `adm_inventory_item_data` row that referenced that field and every `adm_inventory_field_options` entry. The handler validates only a session-bound CSRF token; there is no `isAdministratorInventory()` check at the controller level, and `Admidio\Inventory\Entity\ItemField::delete()` does not enforce one at the entity level either (unlike its sibling `ItemField::save()`, which does check `\$gCurrentUser->isAdministrator()`). Any user who can log in to the site can permanently destroy a non-system inventory field by sending one POST. Version 5.0.10 provides an updated fix.	2026-08-12	6.5	CVE-2026-47233
Admidio--admidio	Admidio is an open-source user management solution. `modules/registration.php` mode `send_login` regenerates a random password for `user_uuid_assigned`, stores its bcrypt hash in `adm_users usr_password`, and emails the cleartext to that user. Every other state-changing mode in the same file (`assign_member`, `assign_user`, `delete_user`, `create_user`) calls `SecurityUtils::validateCsrfToken(\$_POST['adm_csrf_token'])` first; the `send_login` branch does not. Prior to version 5.0.10, page visited by a registration-administrator can issue the request as a top-level navigation, the browser sends the admin's `SameSite=Lax` cookies, and the server resets the chosen user's password without any further interaction from the admin. Version 5.0.10 fixes the issue.	2026-08-12	5.2	CVE-2026-47228
Admidio--admidio	Admidio is an open-source user management solution. Prior to version 5.0.10, `modules/sso/clients.php` validates an `adm_csrf_token` on every state-changing branch except `enable`. The `enable` case loads the SAML or OIDC client by UUID, calls `\$client->enable(\$enabled)`, and persists the new state with no token check. Because the action is reachable via plain GET parameters, a third-party page can	2026-08-12	5.4	CVE-2026-47229

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	trick an authenticated administrator into disabling (or silently re-enabling) any configured SAML or OIDC client. Disabling an SSO client breaks every downstream relying-party application that authenticates through it. Version 5.0.10 contains a fix.			
Admidio--admidio	Admidio is an open-source user management solution. Prior to version 5.0.10, the sensitive `mode=export` action in `modules/sso/keys.php` exports a PKCS#12 bundle containing the configured private key and certificate, but the CSRF validation line is commented out. A forged cross-site POST from an administrator session can therefore trigger private key export without a valid form token. Version 5.0.10 contains a fix.	2026-08-12	4.3	CVE-2026-47232
Admidio--admidio	Admidio is an open-source user management solution. Prior to version 5.0.10, when debug logging is enabled, `Session::setCookie()` logs full cookie values and `Session::start()` logs the current session ID. In a real Admidio deployment this includes both the active session cookie and the persistent auto-login cookie. Anyone with access to the log sink can recover live bearer-style credentials from the logs. Version 5.0.10 contains a fix.	2026-08-12	4.4	CVE-2026-47234
Adobe--Adobe Commerce	Adobe Commerce is affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker with high privileges could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue does not require user interaction.	2026-08-11	6.5	CVE-2026-48411
Adobe--ColdFusion 2025	ColdFusion is affected by an Incorrect Authorization vulnerability that could result in an application denial-of-service. A low-privileged attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	6.5	CVE-2026-48375
Adobe--ColdFusion 2025	is affected by an Improper Encoding or Escaping of Output vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain limited unauthorized write access, causing a limited disruption to availability. Exploitation of this issue does not require user interaction.	2026-08-11	5.4	CVE-2026-48376
Adobe--ColdFusion 2025	is affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-08-11	4.6	CVE-2026-21269
Adobe--ColdFusion 2025	ColdFusion is affected by an Improper Input Validation vulnerability that could result in an application denial-of-service. An attacker with high privileges could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	4.9	CVE-2026-48384
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Integer Overflow or Wraparound vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	6.2	CVE-2026-48387
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	6.2	CVE-2026-48434
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	6.2	CVE-2026-48435

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	2026-08-11	6.5	CVE-2026-48436
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	6.2	CVE-2026-48443
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Integer Overflow or Wraparound vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	6.2	CVE-2026-48444
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Integer Overflow or Wraparound vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	6.2	CVE-2026-48445
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-11	6.2	CVE-2026-71389
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Improper Certificate Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	2026-08-11	5.5	CVE-2026-48437
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	2026-08-11	5.5	CVE-2026-48446
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in privilege escalation. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-08-11	4.7	CVE-2026-47922
Adobe--Content Credentials Rust SDK	CAI Content Credentials is affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized limited write access. Exploitation of this issue does not require user interaction.	2026-08-11	4	CVE-2026-71390
AfterShip & Automizely--AfterShip Tracking	Subscriber Cross Site Scripting (XSS) in AfterShip Tracking <= 1.18.1 versions.	2026-08-13	6.5	CVE-2026-66460
aliakro--Snippet Shortcodes	The Snippet Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 5.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-16	6.4	CVE-2026-16758

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alian--Astro Booking Engine	The Astro Booking Engine plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.0. This is due to missing nonce validation on the options deletion functionality. This makes it possible for unauthenticated attackers to delete all plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-08-14	4.3	CVE-2025-10308
alldatacenter--alldata	A flaw has been found in alldatacenter alldata up to 0.6.8. This impacts the function FileInputStream of the file /admin/controller/JobLogController.java of the component logDetailCat Endpoint. This manipulation of the argument executorAddress causes path traversal. It is possible to initiate the attack remotely. The exploit has been published and may be used. The project closed the issue report as "not planned" without any further explanation.	2026-08-14	5.3	CVE-2026-19827
Aonetheme--Service Finder Booking	Subscriber Broken Access Control in Service Finder Booking <= 6.2 versions.	2026-08-13	6.5	CVE-2026-28159
Apioo--Fusio	A server-side request forgery vulnerability in Apioo Fusio 8.8.3 allows authenticated consumer-role users to make the server issue HTTP requests to internal network addresses by registering a webhook URL pointing to an internal host. The webhook registration endpoint validates URL syntax via FILTER_VALIDATE_URL but applies no IP or host denylist. When the registered event fires, the server issues an HTTP POST to the attacker-supplied internal URL.	2026-08-11	6.5	CVE-2026-72598
aresit--WP Compress Instant Performance & Speed Optimization	The WP Compress - Instant Performance & Speed Optimization plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 7.10.09. This is due to missing or incorrect nonce validation on the (top-level template code) function. This makes it possible for unauthenticated attackers to delete arbitrary WordPress options, including critical ones such as siteurl, home, active_plugins, template, and stylesheet, causing site outage or a full plugin and theme reset via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-08-16	6.5	CVE-2026-17608
Arraytics--WP Event SOLUTION	Customer Sensitive Data Exposure in WP Event SOLUTION <= 4.1.18 versions.	2026-08-13	6.5	CVE-2026-28174
Attendize--Attendize	An improper authorization vulnerability in Attendize through commit 9289acb allows an authenticated remote attacker to inject persistent mandatory survey questions into another organizer's events via the POST /event/{event_id}/question/create endpoint. The postCreateEventQuestion method loads the target event without the tenant-isolation scope, enabling cross-tenant writes; the injected question cannot be removed by the victim because the victim's account-scoped delete path cannot resolve a question owned by another tenant.	2026-08-10	5.4	CVE-2026-72690
Autodesk--Installer	A maliciously crafted input, when processed by the Autodesk Installer IPC frame parser, may trigger improper validation of an input-specified position or offset, resulting in an out-of-range substring operation. A malicious actor may leverage this vulnerability to cause the NT AUTHORITY\SYSTEM service to terminate unexpectedly, resulting in a denial-of-service condition.	2026-08-12	5.5	CVE-2026-14479
Automattic--mongoose	Mongoose is a MongoDB object modeling tool designed to work in an asynchronous environment. Prior to 6.13.10, 7.8.10, 8.24.1, and 9.7.2, passing a user-controlled update such as MyModel.updateOne(filter, req.body) can exploit Mongoose update casting with a __proto__.x dotted path under \$set. Schema.prototype.path and Schema.prototype._getPathType can treat inherited properties of schema.paths and schema.nested as schema types, allowing the casting process to set \$fullPath and \$parentSchemaDocArray on Object.prototype before throwing. This prototype pollution makes those properties visible on newly	2026-08-13	6.5	CVE-2026-73562

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	created objects and can cause application integrity and availability impacts. This issue is fixed in versions 6.13.10, 7.8.10, 8.24.1, and 9.7.2.			
AWS--aws-sdk-cpp	An out-of-bounds write issue in the Base64 decoder in Amazon aws-sdk-cpp before 1.11.862 might allow a remote authenticated user to cause a crash or heap memory corruption in an application that processes crafted Base64-encoded input. To remediate this issue, users should upgrade to version 1.11.862.	2026-08-12	5.9	CVE-2026-19642
AWS--aws-sdk-cpp	An out-of-bounds read issue in the Base64 decoder in Amazon aws-sdk-cpp before 1.11.862, on some platforms, might allow a remote authenticated user to crash an application that processes crafted Base64-encoded input. To remediate this issue, users should upgrade to version 1.11.862.	2026-08-12	5.3	CVE-2026-19643
Axis Communications AB--AXIS OS	The ACAP framework contains a Time-of-Check to Time-of-Use (TOCTOU) race condition, which could potentially lead to privilege escalation. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	2026-08-11	5.7	CVE-2026-5303
Axis Communications AB--AXIS OS	An ACAP configuration file lacks input validation, which could potentially lead to privilege escalation. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	2026-08-11	5.7	CVE-2026-5304
Axis Communications AB--AXIS OS	The Device Configuration Framework is vulnerable to an authentication bypass flaw. This flaw can only be exploited after authenticating with a viewer-privileged service account.	2026-08-11	5.9	CVE-2026-6181
Axis Communications AB--AXIS OS	The ACAP framework contains a Time-of-Check to Time-of-Use (TOCTOU) race condition, which could potentially lead to privilege escalation. This vulnerability can only be exploited if the Axis device is configured to allow the installation of unsigned ACAP applications, and if an attacker convinces the victim to install a malicious ACAP application.	2026-08-11	5.1	CVE-2026-6505
Axis Communications AB--Signed Video Framework	The Signed Video Framework contained a buffer overflow issue which could lead the application using this framework to crash. The issue exclusively affects the tools used for the validation of signed content. The AXIS OS device's signed video functionality remains unaffected.	2026-08-11	5.3	CVE-2026-8158
backstage--backstage	Backstage is an open framework for building developer portals. Prior to 0.29.2, the experimental dynamic client registration and client ID metadata document features in the @backstage/plugin-auth-backend use full-string matcher.isMatch glob matching for auth.experimentalDynamicClientRegistration.allowedRedirectUriPatterns and the auth.experimentalClientIdMetadataDocuments allowedClientIdPatterns and allowedRedirectUriPatterns options. A hostname wildcard can match across URL component boundaries, allowing an attacker-controlled redirect URI with a trusted hostname suffix in its path to pass the allowlist and receive an OAuth authorization code after a victim completes the flow. Patterns without an explicit protocol can match unintended protocols, and redirect URIs containing embedded credentials are accepted after user information is stripped for matching. The features are experimental and disabled by default; only deployments that enable them and configure custom wildcard-hostname or protocol-less patterns are affected. This issue is first fixed in prerelease version 0.29.2.	2026-08-13	4.7	CVE-2026-73563
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Prior to version 3.17.0, Typebot's WhatsApp status forwarding feature stores a workspace-configured webhook forwarding URL and later POSTs WhatsApp marketing/error status events to it from the server. The stored URL is only validated as a generic URL in settings, but the forwarding code uses the raw `ky` instance instead of the repository's SSRF-protected `safeKy` client. A workspace user who can configure WhatsApp settings can therefore make the Typebot server issue HTTP requests to internal services, private-network hosts,	2026-08-11	5.4	CVE-2026-48483

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	localhost, or metadata-style endpoints whenever the public WhatsApp production webhook receives a status payload that should be forwarded. Version 3.17.0 patches the issue.			
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Prior to version 3.16.0, the OpenAI "Create Transcription" action handler fetches a user-supplied audio URL using `fetch()` without applying the SSRF protection that exists elsewhere in the codebase. An attacker can direct the server to make HTTP requests to arbitrary internal addresses and localhost. The fetched content is passed to the OpenAI Whisper API and the transcription result is returned to the attacker. Version 3.16.0 fixes the issue.	2026-08-11	5.4	CVE-2026-48762
basecamp--trix	Trix is a what-you-see-is-what-you-get rich text editor for everyday writing. Prior to 2.1.18, Trix is vulnerable to stored cross-site scripting when crafted HTML is pasted into the editor. HTMLParser processes a mock attachment in a ` <span>` with an empty `data-trix-attachment="{}"` value, causing data-trix-attributes to be applied to a plain string piece. StringPiece.fromJSON accepts an unvalidated href, allowing a javascript: URI to enter the document model and serialized HTML and execute when another user renders and clicks the content. Applications that apply server-side HTML sanitization can neutralize the payload on save. This issue is fixed in version 2.1.18.	2026-08-13	4.6	CVE-2026-73428
Bash-it--Bash-it	Bash-it 3.2.0 contains a terminal escape sequence injection vulnerability in the barbuk theme's Python virtualenv prompt segment that allows local attackers to inject arbitrary terminal control sequences by embedding escape sequences in the requires-python field of a pyproject.toml file. When a user navigates into a directory containing a maliciously crafted pyproject.toml, the unfiltered field value is read via awk and concatenated directly into PS1 through __prompt-command without stripping control characters, causing injected OSC or CSI sequences to be written to and interpreted by the terminal emulator on every prompt render.	2026-08-11	4.4	CVE-2026-73036
beaverbuilder--Beaver Builder Page Builder Drag and Drop Website Builder	The Beaver Builder Page Builder - Drag and Drop Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Button Module 'button' (Button Code) Setting in all versions up to, and including, 2.10.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Beaver Builder grants editor access to any WordPress role holding the edit_posts capability by default, meaning Author-level users and above can exploit this vulnerability.	2026-08-15	6.4	CVE-2026-17090
bestwebsoft--Profile Extra Fields by BestWebSoft	Subscriber Cross Site Scripting (XSS) in Profile Extra Fields by BestWebSoft <= 1.3.4 versions.	2026-08-13	6.5	CVE-2026-66456
bitpressadmin--Bit Form Contact Form, Payment Forms, Multi Step Forms, Calculator & Custom Form Builder	The Bit Form - Contact Form, Payment Forms, Multi Step Forms, Calculator & Custom Form Builder plugin for WordPress is vulnerable to generic SQL Injection via the 'data[queryCondition]' parameter in all versions up to, and including, 3.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-14	6.5	CVE-2026-16810
bitwarden--server	Bitwarden Server before 2026.7.2 does not verify that the caller is a member of the organization identified in a POST /collect request body, allowing any authenticated user to write forged, arbitrarily backdated entries into any organization's audit log.	2026-08-10	5.8	CVE-2026-71959
Bludit--Bludit	A stored cross-site scripting (XSS) vulnerability in Bludit 4.0.0-beta allows a low-privileged authenticated user (Author role) to inject arbitrary JavaScript by	2026-08-10	5.4	CVE-2026-72576

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	uploading a crafted SVG file as the site logo. A stored script tag in the SVG executes in the browser of any user who loads the logo.			
bluewave-labs--Checkmate	A user enumeration vulnerability in bluewave-labs/Checkmate through 2.1.0 allows an unauthenticated remote attacker to determine whether a given email address is registered. The POST /api/v1/auth/recovery/request endpoint returns HTTP 200 for registered email addresses and a different status code for unregistered ones, enabling attackers to enumerate valid user accounts.	2026-08-10	5.3	CVE-2026-72588
boldthemes--Bold Page Builder	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'bt_bb_shortcode' shortcode in all versions up to, and including, 5.6.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-16	6.4	CVE-2026-2357
brainstormforce--SureDash Community, Courses & Member Dashboard	The SureDash - Community, Courses & Member Dashboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'draweropenverposition' Block/Shortcode Attribute in all versions up to, and including, 1.10.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected payload is stored inside the block-delimiter HTML comment's JSON, which wp_kses_post does not neutralize on save, and is only interpolated into the rendered style attribute at display time without esc_attr() escaping, allowing a double-quote to break out of the attribute and introduce arbitrary HTML event handlers.	2026-08-16	6.4	CVE-2026-18402
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.25, POST /api/global/auth/:tenantId/login incremented the failure counter in packages/worker/src/api/controllers/global/auth.ts only for existing users, while packages/worker/src/middleware/emailLockout.ts returned X-Account-Locked and Retry-After only for locked identifiers. An unauthenticated attacker could compare the response after repeated failures to enumerate valid email addresses and temporarily lock valid accounts. This issue is fixed in version 3.39.25.	2026-08-12	5.3	CVE-2026-73306
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.25, packages/server/src/api/controllers/automation.ts returned automation test results containing trigger.outputs.user.oauth2, broadcast BuilderSocketEvent.AutomationTestProgress to the app room, and stored progress in packages/server/src/automations/testProgress.ts without user scoping. A co-builder could receive or poll another SSO-authenticated builder test and obtain OAuth2 access and refresh tokens. The fix adds sanitizeAutomationTestResult and isolates progress by user. This issue is fixed in version 3.39.25.	2026-08-12	5.7	CVE-2026-73308
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.25, the GET /api/global/groups endpoint in packages/worker/src/api/routes/global/groups.ts omitted auth.builderOrAdmin, allowing an authenticated BASIC role user to enumerate tenant groups, role mappings and user memberships, builder permissions, and default-group flags. The disclosure exposes the tenant access-control structure to users who are not builders or administrators. This issue is fixed in version 3.39.25.	2026-08-12	4.3	CVE-2026-73301
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.25, GET /api/users/metadata and GET /api/users/metadata/:id returned user objects processed by packages/server/src/utilities/global.ts without removing oauth2.accessToken or oauth2.refreshToken. A user with the POWER role could retrieve the identity-provider credentials of SSO-authenticated users and use the refresh tokens for persistent access to connected services. This issue is fixed in version 3.39.25.	2026-08-13	4.9	CVE-2026-73304

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
buildwps--PPWP Password Protect Pages	The PPWP - Password Protect Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's `ppwp` shortcode attributes in all versions up to, and including, 1.9.21 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-13	6.4	CVE-2026-3639
buildwps--PPWP Password Protect Pages	The PPWP - Password Protect WordPress #1 Most-Reviewed Password Plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.9.20 via the ppw_free_set_password AJAX action due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Contributor-level access and above, to update the password on any password protected post and subsequently access the content.	2026-08-16	4.3	CVE-2025-10005
buildwps--Prevent Direct Access Protect WordPress Files	The Prevent Direct Access - Protect WordPress Files plugin for WordPress is vulnerable to unauthorized access of protected files due to insufficient token validation in the `get_advance_file_by_url()` method in all versions up to, and including, 2.8.8.8 The method uses a SQL `LIKE` operator for token lookup without escaping wildcard characters via `\$wpdb->esc_like()`. This makes it possible for unauthenticated attackers to bypass the private token requirement by supplying SQL wildcard characters (such as `%`) as the token value, matching any record in the plugin's file table and downloading any protected file.	2026-08-13	5.3	CVE-2026-3835
Byron--dua-cli	dua-cli fails to filter terminal escape sequences when printing marked file paths after exiting the TUI interface. Attackers can craft file names containing OSC/CSI escape sequences that are interpreted by the terminal emulator when printed, enabling title spoofing, clipboard manipulation, or other escape-sequence attacks.	2026-08-13	5	CVE-2026-73479
Calix--GigaSpire	A flaw has been found in Calix GigaSpire 26.1.0. Impacted is an unknown function of the file utilities_configurationsave.cgi of the component Web Management Interface. Executing a manipulation of the argument sessionKey can lead to denial of service. The attack can be launched remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-13	4.3	CVE-2026-19745
Calix--GigaSpire	A vulnerability has been found in Calix GigaSpire 26.1.0. The affected element is an unknown function of the file traceroute.cmd. The manipulation leads to denial of service. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-13	4.3	CVE-2026-19746
Canonical--LXD	An authorization bypass vulnerability in LXD allows an authenticated attacker to bypass project-level container isolation restrictions. When a project is configured with restrictions on container privileges (such as enforcing restricted.containers.privilege=isolated), LXD fails to enforce the requirement if an instance configuration omits the security.idmap.isolated key. An attacker can exploit this flaw by creating or updating an instance without explicitly setting security.idmap.isolated, bypassing the target project's security constraints.	2026-08-12	4.3	CVE-2026-63295
CapSoftware--Cap	Cap v0.3.1 contains a broken access control vulnerability in the POST /api/video/comment endpoint that allows authenticated users to post comments on any private video without permission by supplying an arbitrary videoid in the request body. Attackers can inject comments into private video recordings belonging to other users, trigger comment notification emails to the video owner, and enumerate valid video IDs through response differences.	2026-08-11	5.4	CVE-2026-69113
capstone-engine--capstone	Capstone is a disassembly framework. Prior to version 6.0.0-Alpha9, Capstone's public `cs_insn_name()` API forwards caller-supplied instruction IDs directly to the selected architecture backend. Most backends validate the ID before indexing instruction-name tables, but the M68K and RISCv backends have missing or incomplete bounds checks. On a Capstone handle opened for M68K or RISCv, a	2026-08-14	5.1	CVE-2026-49282

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	caller-controlled invalid instruction ID can trigger an out-of-bounds read and crash the process. The demonstrated impact is availability loss in applications or bindings that expose instruction-name lookup to untrusted IDs. No code execution or data disclosure was demonstrated. Version 6.0.0-Alpha9 patches the issue.			
chatwoot--chatwoot	Chatwoot is a customer engagement suite. Prior to 4.9.0, Chatwoot allowed authenticated account administrators to transfer Portals, Automation Rules, Macros, and Twilio Channels to other accounts through the writable account_id parameter. This could break tenant isolation and cause cross-account data exposure, unauthorized configuration changes, or loss of access to transferred resources. This issue is fixed in version 4.9.0.	2026-08-10	6.7	CVE-2026-72719
cisagov--Malcolm	Malcolm is a network traffic analysis tool suite. Prior to version 26.07.0, `safe-extract.py` extracts uploaded archives with no limit on entry count, directory depth, total entries, or output size. A small malicious archive containing a large number of directory or file entries causes the filebeat processing container to create an unbounded number of filesystem objects, exhausting inodes or filesystem metadata and denying service to the processing pipeline and any service sharing the same mount. Version 26.07.0 fixes the issue.	2026-08-11	6.5	CVE-2026-63133
cisagov--Malcolm	Malcolm is a network traffic analysis tool suite. Prior to version 26.07.0, `safe-extract.py` protects file extraction with libarchive's secure flags, but creates directory entries with a raw `os.makedirs(os.path.join(dest, entry.pathname))` that has no traversal protection. An uploaded malicious archive containing a directory entry with a `../` sequence or an absolute path causes the filebeat processing container to create directories outside the intended extraction directory. Version 26.07.0 fixes the issue.	2026-08-11	5.4	CVE-2026-63134
civetweb--civetweb	CivetWeb (commit 4a4f0c95) contains a heap and stack buffer overflow vulnerability in the read_websocket() function that allows unauthenticated remote attackers to corrupt memory by sending compressed WebSocket frames when both USE_ZLIB and MG_EXPERIMENTAL_INTERFACES are defined. Attackers can negotiate permessage-deflate during the WebSocket handshake and send a crafted frame with the RSV1 bit set, causing the server to write a 4-byte zlib sync trailer out-of-bounds past the allocated buffer, leading to heap metadata corruption, denial of service, or potential code execution.	2026-08-11	6.5	CVE-2026-29035
code-projects--Online Food Order System	A flaw has been found in code-projects Online Food Order System 1.0. The impacted element is an unknown function of the file delete_food_items1.php. Executing a manipulation of the argument checkbox can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	2026-08-15	6.3	CVE-2026-19917
code-projects--Online Shopping System	A vulnerability was determined in code-projects Online Shopping System 1.0. Affected is an unknown function of the file /action.php. This manipulation of the argument prold causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-15	6.3	CVE-2026-19920
code-projects--Online Shopping System	A vulnerability was identified in code-projects Online Shopping System 1.0. Affected by this vulnerability is an unknown functionality of the file /homeaction.php. Such manipulation of the argument cat_id leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2026-08-16	6.3	CVE-2026-19921
code-projects--Online Shopping System	A weakness has been identified in code-projects Online Shopping System 1.0. This affects an unknown part of the file /checkout_process.php. Executing a manipulation of the argument total_count can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-16	6.3	CVE-2026-19923
composefs--tar-rs	tar-rs versions 0.4.11 through 0.4.46 contain a symlink escape vulnerability in the Builder::append_dir_all() function that allows attackers to read files outside the intended source root directory by planting symlinks in an attacker-controlled	2026-08-10	6.5	CVE-2026-70622

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	directory. When a privileged process archives an untrusted directory, the function follows symlinks without verifying that resolved targets remain within the source root, causing out-of-bounds files to be included in the archive as regular files and disclosed to the attacker.			
contest-gallery--Contest Gallery Upload & Vote Photos, Media, Sell with PayPal & Stripe	The Contest Gallery - Upload & Vote Photos, Media, Sell with PayPal & Stripe plugin for WordPress is vulnerable to Second-Order SQL Injection via MultipleFiles Second-Order Payload via 'cg_multiple_files_for_post' -> 'cgRealld' in all versions up to, and including, 30.0.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-15	6.5	CVE-2026-16586
CoreBunch--Instatic	A cache poisoning vulnerability in CoreBunch/Instatic through 0.0.14 allows an unauthenticated remote attacker to poison the shared process-wide render cache by manipulating the u query parameter of the GET /_instatic/hole/<nodeId> server island endpoint.	2026-08-10	6.1	CVE-2026-72587
coturn--coturn	Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.17.0, shutdown_client_connection() in src/server/ns_turn_server.c prematurely calls dec_quota() and releases bandwidth accounting during the first-stage close of a mobility-enabled allocation while preserving the allocation, relay socket, session, and mobility ticket, allowing an authenticated client to bypass --user-quota and --total-quota and exhaust relay ports. This issue is fixed in version 4.17.0.	2026-08-11	6.5	CVE-2026-73216
craftcms--cms	Craft CMS before 5.10.5 fails to persist updated credential counters after WebAuthn assertion validation in the passkey login endpoint. Attackers can replay captured login request bodies containing requestOptions and response to create additional authenticated sessions for victim accounts.	2026-08-11	6.5	CVE-2026-72780
craftcms--cms	Craft CMS versions >= 5.0.0-RC1 before 5.10.6 and >= 4.0.0-RC1 before 4.18.2 interpolate environment variables and secrets (via \${ENV_VAR} strings in the elementId parameter) into Twig templates before rendering, even when the Twig sandbox is enabled. An authenticated attacker with control panel access can render a malicious sandboxed Twig template and, using a blind error-based technique across many requests, incrementally leak arbitrary environment variables and secrets. These can be abused to forge sessions (via CRAFT_SECURITY_KEY), escalate privileges, and steal database, SMTP, API, or blob storage credentials. Fixed in 5.10.6 and 4.18.2.	2026-08-11	6.5	CVE-2026-72782
craftcms--cms	Craft CMS versions >= 5.0.0-RC1 before 5.10.6 and >= 4.0.0-RC1 before 4.18.2 contain a theoretical path traversal weakness in the ensurePathIsContained function of the Local file system class. The order of operations validates the path before normalization, so normalization could invalidate prior validation assumptions (a desanitization-style issue) and potentially resolve to files outside the intended volume directory. The vendor notes the issue is not directly exploitable and no exploitable scenario has been discovered; the fix is recommended for hardening.	2026-08-11	6.2	CVE-2026-72783
craftcms--cms	Craft CMS versions before 5.10.8 contain an authentication bypass vulnerability in the elements/save action that allows authenticated users to change passwords without verification. Attackers with edit users permission can reset any user's password including administrators by exploiting the unprotected newPassword field in the User element save flow.	2026-08-12	6.5	CVE-2026-72786
craftcms--cms	Craft CMS versions before 5.10.8 contain a stored cross-site scripting vulnerability in the control panel where draft names are rendered without HTML encoding in element chips and cards. A low-privilege user who can create element drafts can inject malicious JavaScript that executes in the browser of any higher-privileged	2026-08-12	6.4	CVE-2026-72787

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user viewing the affected element, allowing account creation and other authenticated actions.			
craftcms--cms	Craft CMS versions >= 5.0.0-RC1 before 5.10.6 and >= 4.0.0-RC1 before 4.18.2 contain a server-side request forgery vulnerability in the GraphQL save<Volume>Asset mutation, which fetches an attacker-supplied URL server-side. The anti-SSRF validation is incomplete: validateIp() does not cover CGNAT (100.64.0.0/10) or NAT64 (64:ff9b::/96) ranges, and the only IP check runs after the request has already been issued. An attacker holding a GraphQL token scoped only to asset-creation permissions can disclose internal HTTP content from CGNAT/NAT64 targets, force outbound GET requests to internal hosts (including RFC1918, loopback, and metadata endpoints), and enumerate internal services.	2026-08-11	5.4	CVE-2026-72784
craftcms--cms	Craft CMS 5.0.0-RC1 before 5.10.6 and 4.0.0-RC1 before 4.18.2 contain an arbitrary file read vulnerability. The create() Twig function restricts class instantiation using a 5-entry blocklist that does not include SplFileObject, allowing an authenticated administrator (with allowAdminChanges=true) to configure a malicious entry type title or URI format that instantiates SplFileObject in a non-sandboxed template context. When a user subsequently creates an entry in the affected section, arbitrary files on the server (such as .env containing the security key and database credentials) are read and rendered as entry titles.	2026-08-11	4.5	CVE-2026-72779
craftcms--cms	Craft CMS 5.0.0-RC1 through 5.10.5 contains an incorrect authorization vulnerability. A control-panel user holding only the viewCategories permission (without saveCategories) for a category group can permanently modify that group's category structure - reordering and re-parenting categories - via the structures/move-element action. The structureEditable flag is computed from the view permission rather than the save permission, and the StructuresController authorizes the mutating action on that read-time session grant without a save re-check. Because a category's URI is derived from its position in the structure, moving a category changes its URL and those of its descendants and can corrupt navigation menus built from the category taxonomy. The issue is fixed in 5.10.6.	2026-08-11	4.3	CVE-2026-72785
croixhaug--Simply Schedule Appointments	The Appointment Booking Calendar - Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.6.12.10 via the ssa_past_appointments due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to access appointment records belonging to arbitrary users and harvest the per-appointment ownership tokens (32-character hashes) embedded in the rendered HTML, which can then be used without any authentication to read or modify those appointments including full customer PII such as name, email, phone number, and private notes. The /wp-json/ssa/v1/render-shortcode REST endpoint is registered unconditionally on rest_api_init regardless of whether the Divi theme is installed, and its permission callback only requires current_user_can('edit_posts'), meaning any Contributor-level account is sufficient to trigger this entire exploit chain.	2026-08-16	6.5	CVE-2026-13358
cryout-creations--Serious Slider	The Serious Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'theme' Shortcode Attribute in all versions up to, and including, 1.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-16	6.4	CVE-2026-15726
cservit--affiliate-toolkit Multi-Network Affiliate & Amazon Product Display	The affiliate-toolkit - Multi-Network Affiliate & Amazon Product Display plugin for WordPress is vulnerable to time-based SQL Injection via the 'orderby' parameter in all versions up to, and including, 3.8.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access	2026-08-14	4.9	CVE-2026-12743

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.			
cube-root--directory-serve	A stored cross-site scripting (XSS) vulnerability in cube-root/directory-serve through 1.3.7 allows an attacker to inject arbitrary JavaScript into the web interface by uploading a file with a crafted filename containing HTML attribute-breaking characters.	2026-08-10	5.4	CVE-2026-72570
Daniel Brendel--HortusFox	A stored cross-site scripting vulnerability in HortusFox 5.9 allows authenticated workspace members to inject persistent JavaScript into plant notes via Parsedown rendered without safe mode. Notes are rendered unescaped in the browser of every user who views the affected plant. An attacker can use this to steal session cookies or perform actions in the context of other users including administrators.	2026-08-11	5.4	CVE-2026-72559
dartiss--draft-list	Draft List is a WordPress plugin to manage and promote unpublished content. Versions 2.6.3 and below are vulnerable to stored Cross-Site Scripting (XSS) in the `[drafts]` shortcode and Draft List widget when the documented custom `template` option places the `{{draft}}` placeholder inside an HTML attribute. The vulnerable code inserts the raw draft `post_title` into `{{draft}}` when the current viewer cannot edit posts. Because the template is sanitized before `{{draft}}` replacement, a Contributor can store a quote-only title payload that breaks out of an attribute in a site-configured Draft List template and executes JavaScript for visitors who load the public page. Version 2.6.4 fixes the issue.	2026-08-12	6.5	CVE-2026-49466
dataease--SQLBot	SQLBot through 1.10.0, fixed in commit c3f40a5, contains a stored cross-site scripting vulnerability in the SQText dashboard component that renders TinyMCE output via v-html without sanitization. Attackers who can modify dashboard text widget content can inject arbitrary HTML and JavaScript that executes for all users viewing the dashboard.	2026-08-10	5.4	CVE-2026-72743
DayuanJiang--next-ai-draw-io	Next AI Draw.io 0.2.1 through 0.4.16 contains a reflected cross-site scripting vulnerability in the mcp query parameter that is interpolated without escaping into HTML and JavaScript. Attackers can craft malicious URLs to execute arbitrary JavaScript in the localhost origin, enabling exfiltration of diagram sessions and API data.	2026-08-13	6.1	CVE-2026-73037
DefaultFuction--Customer-Relationship-Management-In-C-Project	A weakness has been identified in DefaultFuction Customer-Relationship-Management-In-C-Project 2.0. Impacted is the function gets of the component Customer Search Module. This manipulation causes stack-based buffer overflow. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The project confirms, that "it's being processed".	2026-08-16	6.3	CVE-2026-19933
DefaultFuction--Notice-System-Managent	A security flaw has been discovered in DefaultFuction Notice-System-Managent 2.0. This issue affects the function GroovyShell.evaluate of the file /execute of the component NoticeController. The manipulation results in code injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The project confirms, that "it's being processed".	2026-08-16	6.3	CVE-2026-19932
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to 2605.0.2, contain an Improper Deserialization of Untrusted Data vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Privilege Escalation.	2026-08-14	6.3	CVE-2026-63701
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to 2605.0.2, contain a Use of Hard-coded Credentials vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-08-14	6.3	CVE-2026-63702
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to 2605.0.2, contain a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with	2026-08-14	5.3	CVE-2026-66272

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote access could potentially exploit this vulnerability, leading to Information disclosure.			
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.7, 2026.6.2, 2026.7.1, and 2026.8.0-latest.1, Discourse has HTML injection in PrettyText.format_for_email because cooked attribute values are reparsed as markup. Crafted Vimeo iframe sources, secure-upload URLs or dimensions, and hashtag data-slug values can cause decoded attribute text to be reinterpreted as HTML. The vulnerable conversion also fails to strictly validate the Vimeo iframe host and path, allowing non-Vimeo allowlisted iframes to be converted. This issue is fixed in versions 2026.1.7, 2026.6.2, 2026.7.1, and 2026.8.0-latest.1.	2026-08-10	6.4	CVE-2026-72720
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, an authenticated user could eavesdrop on private AI bot conversations through the AI bot reply stream. The issue is fixed in 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-10	6.5	CVE-2026-72726
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.7, an authenticated user could submit specially formed URLs that bypassed the Onebox allowlist and embedded malicious content in a site. This issue is fixed in versions 2026.1.7, 2026.6.2, 2026.7.1, and 2026.8.0-latest.1.	2026-08-10	6.3	CVE-2026-72728
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, Onebox::DomainChecker.is_blocked? compares hostnames and SiteSetting.blocked_onebox_domains entries case-sensitively, allowing an attacker to bypass configured Onebox domain restrictions by changing character casing in a redirect target hostname. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-10	5.3	CVE-2026-72721
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, SiteSerializer.anonymous_default_navigation_menu_tags serializes tags from SiteSetting.default_navigation_menu_tags without applying DiscourseTagging.filter_visible for the anonymous viewer. An unauthenticated user can retrieve restricted tag names and descriptions through /site.json when those tags are limited by inaccessible categories, category tag groups, or tag-group permissions. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-10	5.3	CVE-2026-72723
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, the staff action log model rendered unescaped previous and new value fields that could inject stored cross-site scripting into the staff interface. The issue is fixed in 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-10	5.4	CVE-2026-72725
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, TopicLink.extract_from, TopicLink.ensure_entry_for, and TopicLink.duplicate_lookup do not consistently enforce Guardian.can_see? checks when processing internal links. An authenticated user can submit links to restricted topics, private messages, or hidden posts and receive canonicalized slugs or titles in the composer_messages duplicate_lookup response even though the targets are not visible to that user. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-10	4.3	CVE-2026-72722
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, plugins/chat/lib/chat/onebox_handler.rb resolves Chat::Thread by route thread_id independently of the route channel_id before checking whether the user can preview the selected chat channel. An authenticated user can pair a public channel ID with a private thread ID in a /onebox.json request and obtain private thread message content. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-10	4.3	CVE-2026-72724

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, the discourse_templates endpoint exposed hidden tag names because DiscourseTemplates::TemplatesSerializer in plugins/discourse-templates/app/serializers/discourse_templates/templates_serializer.rb did not filter tags through the request Guardian. The serializer did not respect tag group permissions, allowing users to see tags they were not permitted to view. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-10	4.3	CVE-2026-72732
django-helpdesk--django-helpdesk	django-helpdesk before 2.3.3 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject arbitrary JavaScript by submitting HTML-formatted email messages or uploading .html/.htm file attachments through public ticket submission channels. Attackers can exploit the lack of sanitization and Content-Disposition headers at the attachment-serving layer to execute malicious scripts in the browser session of authenticated staff members who open the attachment while triaging tickets.	2026-08-13	6.1	CVE-2026-73531
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, the createCommand() function constructs shell commands by interpolating compose service names and configuration into bash command strings. When a compose with a maliciously crafted name or service definition is deployed, the shell metacharacters are interpreted as command separators, allowing arbitrary command execution on the Docker host. This vulnerability is fixed in 0.29.13.	2026-08-10	6.5	CVE-2026-72739
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.13, application.one in apps/dokploy/server/api/routers/application.ts returns provider relations loaded by findApplicationById in packages/server/src/services/application.ts without redacting githubClientSecret, githubPrivateKey, or githubWebhookSecret, allowing a user with only service:read permission to retrieve another user's Git provider secrets even when hasGitProviderAccess is false and unauthorizedProvider is set. This issue is fixed in version 0.29.13.	2026-08-10	6.5	CVE-2026-72873
Dolibarr--Dolibarr	A security flaw has been discovered in Dolibarr up to 23.0.3. Affected is an unknown function of the file htdocs/user/card.php of the component User Cloning. The manipulation of the argument ID results in ldap injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The patch is identified as 798e65356ede03c2812ab1a728f23fae34de5592. It is advisable to implement a patch to correct this issue.	2026-08-16	6.3	CVE-2026-19930
dotonpaper--Pinpoint Booking System Version 2	The Pinpoint Booking System - Version 2 plugin for WordPress is vulnerable to Price Manipulation via the `cart_data` parameter in all versions up to, and including, 2.9.9.6.8. This is due to the `dopbsp_woocommerce_add_to_cart` AJAX action being registered via `wp_ajax_nopriv_*` with no authentication, no nonce verification, and no server-side recalculation of pricing - the `update` handler reads `price_total` directly from the attacker-controlled `cart_data` POST parameter and persists it to the database via `\$wpdb->insert()` without validating it against the calendar's configured pricing. The `woocommerce_before_calculate_totals` callback subsequently reads the stored attacker-supplied value back from the database and passes it directly to `\$product->set_price()` without recomputing from calendar settings. This makes it possible for unauthenticated attackers to override the WooCommerce checkout price of any bookable product tied to a booking calendar to an arbitrary value, effectively enabling the purchase of any such product at a self-chosen price.	2026-08-15	5.3	CVE-2026-12128
Dromara--lamp-cloud	A vulnerability has been found in Dromara lamp-cloud up to 5.10.0. This affects an unknown part of the file DefGenProjectController.java of the component Code Generator. Such manipulation of the argument outputDir/parent/projectPrefix leads to path traversal. It is possible to launch the attack remotely. The exploit has	2026-08-13	6.3	CVE-2026-19756

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.			
DTStack--Taier	A vulnerability has been found in DTStack Taier 1.4.0. Affected is the function MultipartFile.getOriginalFilename of the file UploadController.java of the component Upload Controller. The manipulation of the argument File leads to path traversal. The attack may be initiated remotely. Upgrading to version 1.5.0 is able to address this issue. The identifier of the patch is 572773c4315e23e51e30115151cb091749a8d03e. It is advisable to upgrade the affected component.	2026-08-13	4.7	CVE-2026-19761
dundee--gdu	gdu fails to strip terminal escape sequences from directory and file names when printing paths after TUI exit. Attackers can craft malicious directory or file names containing escape sequences that are interpreted by the terminal, enabling title spoofing, clipboard manipulation, or other terminal-dependent effects.	2026-08-13	5	CVE-2026-73480
ECOVACS ROBOTICS--Android App "ECOVACS PRO"	Android and iOS apps ECOVACS PRO App improperly validate server certificates. Communication may be retrieved and/or altered.	2026-08-10	4.8	CVE-2026-66410
ECOVACS ROBOTICS--DEEBOT PRO M1	DEEBOT PRO M1 and DEEBOT PRO K1VAC do not validate server certificates in MQTT communications. Operation logs and activity logs stored on the affected products may be retrieved.	2026-08-10	6.5	CVE-2026-66404
ECOVACS ROBOTICS--DEEBOT PRO M1	DEEBOT PRO M1 and DEEBOT PRO K1VAC are configured with weak passwords for their Wi-Fi hotspot networks. The password may be analyzed and obtained to connect to the access point of an affected robot.	2026-08-10	5.3	CVE-2026-66409
ECOVACS ROBOTICS--DEEBOT PRO M1	DEEBOT PRO M1 and DEEBOT PRO K1VAC incorrectly implement authentication algorithm in WebSocket communications. An unauthenticated attacker may connect and operate the affected robot.	2026-08-10	5.3	CVE-2026-66411
ECOVACS ROBOTICS--DEEBOT PRO M1	DEEBOT PRO M1 and DEEBOT PRO K1VAC use wget command with server certificate validation disabled. A man-in-the-middle attack may allow to obtain and/or alter communications of the affected products. As a result, arbitrary code may be executed with the administrative privilege.	2026-08-10	4.8	CVE-2026-66406
ECOVACS ROBOTICS--DEEBOT PRO M1	The root accounts of DEEBOT PRO M1 and DEEBOT PRO K1VAC are configured with weak passwords. Physical access to an affected product may allow to obtain the password of the root account.	2026-08-10	4.6	CVE-2026-66408
Ecwid--Ecwid by Lightspeed Ecommerce Shopping Cart	The Ecwid by Lightspeed Ecommerce Shopping Cart WordPress plugin before 7.0.9 does not perform a capability check or nonce verification on one of its store-management actions, allowing any authenticated user, such as a subscriber, to disconnect the store and take the storefront offline until an administrator reconnects it.	2026-08-13	5.4	CVE-2026-14332
Elastic--Eck Operator	The Elastic Cloud on Kubernetes (ECK) operator reads a list of secret references from an annotation on secrets it manages, and it accepts the namespace recorded in each reference without validating that the reference is authorized for the resource being reconciled. A user whose Kubernetes permissions are limited to their own namespace can write that annotation, trigger a reconcile, and cause the operator to use its cluster-wide secret permissions to copy the contents of a secret from any other namespace into a secret the user can read.	2026-08-13	6.5	CVE-2026-72640
Elastic--Eck Operator	Cleartext Storage of Sensitive Information in an Environment Variable (CWE-526) in Elastic Cloud on Kubernetes (ECK) can lead to information disclosure via Retrieve Embedded Sensitive Data (CAPEC-37). When ECK reconciles a Fleet Server resource that authenticates to Elasticsearch with a service account token, the token is written into the generated workload specification in cleartext rather than being referenced from the Kubernetes Secret that ECK maintains for the other	2026-08-13	6.5	CVE-2026-72648

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	credentials on the same path. Any principal able to read workload specifications in the affected namespace can therefore read a live Elasticsearch credential, even when Kubernetes RBAC does not grant that principal access to Secrets.			
Elastic-- Elasticsearch	Uncontrolled Recursion (CWE-674) in the Elasticsearch wildcard matching helper can lead to a denial of service via Excessive Allocation (CAPEC-130). The matcher used to resolve wildcard patterns against names is implemented recursively and had no bound on recursion depth or on the total number of match operations performed. A search request containing a wildcard pattern with a large number of wildcard groups, evaluated against a sufficiently long name, exhausts the thread stack. Elasticsearch treats a stack overflow as an unrecoverable condition and shuts the node down, so the request terminates the affected node rather than failing gracefully.	2026-08-13	6.5	CVE-2026-72636
Elastic-- Elasticsearch	Uncontrolled Recursion (CWE-674) in Elasticsearch can lead to denial of service via Input Data Manipulation (CAPEC-153). An authenticated user holding only low-privileged index creation permissions can submit a single request containing a specially crafted, malformed custom analysis definition that is resolved recursively without a cycle or depth check, exhausting the thread stack and terminating the affected node.	2026-08-13	6.5	CVE-2026-72638
Elastic-- Elasticsearch	Elasticsearch does not enforce an upper bound on a user-supplied count accepted by a search highlighting option, and the allocation derived from that count is not accounted against any circuit breaker. An authenticated user holding only read privileges on a single searchable index can submit one small search request that causes the node to reserve an excessively large internal data structure. The allocation occurs before the existing highlighting safety limits are evaluated, so memory exhaustion raises a fatal error that terminates the Elasticsearch node process. This results in a denial of service for the affected node and degrades cluster routing and health. The defect is not volumetric and does not depend on the size of the indexed data, so a single request is sufficient.	2026-08-13	6.5	CVE-2026-72639
Elastic-- Elasticsearch	Memory Allocation with Excessive Size Value (CWE-789) in Elasticsearch can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated user holding only read privileges on a single index can submit one small, specially crafted search request that causes an excessively large memory allocation, exhausting the JVM heap and terminating the affected node.	2026-08-13	6.5	CVE-2026-72645
Elastic-- Elasticsearch	Uncontrolled Recursion (CWE-674) in Elasticsearch can lead to denial of service via Serialized Data with Nested Payloads (CAPEC-230). An authenticated user holding only read privileges on a single index can submit one specially crafted search request whose deeply nested structure is processed without a depth limit, exhausting the thread stack and terminating the affected node.	2026-08-13	6.5	CVE-2026-72647
Elastic-- Elasticsearch	Memory Allocation with Excessive Size Value (CWE-789) in the ES QL query processing of Elasticsearch can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated user able to submit ES QL queries could send a specially crafted query whose evaluation allocates an unbounded amount of heap memory, exhausting the available heap on the receiving node and causing the node to become unavailable.	2026-08-13	6.5	CVE-2026-72656
Elastic-- Elasticsearch	Elasticsearch does not validate a size value taken from a user-supplied input before that value is used to reserve memory for an internal data structure. An authenticated user holding only read privileges can submit a single small crafted request to a product API endpoint that causes the node to attempt an excessively large allocation. The resulting memory exhaustion raises a fatal error that terminates the Elasticsearch node process, causing a denial of service for the affected node and degrading cluster health. The defect is not volumetric, so a single request is sufficient regardless of the heap size configured on the target node.	2026-08-13	6.5	CVE-2026-72678

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elastic-- Elasticsearch	Elasticsearch does not apply its configurable input length restriction to a user-supplied pattern accepted by an intervals query. Compiling a deeply nested pattern drives unbounded recursion that exhausts the thread stack and raises a fatal error, terminating the Elasticsearch node process and causing a denial of service for that node. An authenticated user holding only read-only privileges on a single searchable index can trigger the condition with one small search request.	2026-08-13	6.5	CVE-2026-72679
Elastic-- Elasticsearch	A flaw in Elasticsearch allows an authenticated user with the privileges required to invoke the simulate pipeline API endpoint (https://www.elastic.co/docs/api/doc/elasticsearch/operation/operation-ingest-simulate) to submit a request that causes a self-referential data structure to be created. When a specific internal component later processes that structure, the operation recurses without bound and raises a fatal error that is not handled by the surrounding execution path, terminating the affected node process and resulting in a denial of service.	2026-08-13	6.5	CVE-2026-72683
Elastic-- Elasticsearch	A flaw in Elasticsearch allows an authenticated user holding only read privileges to submit a small search request containing a crafted user-supplied input. Processing that input causes a specific internal component to allocate memory without any upper bound, and the allocation occurs outside the scope of the existing memory accounting controls that were intended to constrain it. The resulting out-of-memory condition is fatal and terminates the affected node process, causing a denial of service.	2026-08-13	6.5	CVE-2026-72684
Elastic-- Elasticsearch	A flaw in Elasticsearch allows a low-privileged authenticated user to submit a single request containing a crafted user-supplied input. A specific internal component validates the input using a recursive routine and applies no bound to the length of the value being validated, so the validation causes the thread to exhaust its stack. The resulting fatal error is not handled by the surrounding execution paths and terminates the affected node process, producing a denial of service.	2026-08-13	6.5	CVE-2026-72686
Elastic-- Elasticsearch	A flaw in Elasticsearch allows a low-privileged authenticated user to submit a single small request containing a forged opaque identifier. Elasticsearch decodes and deserializes the identifier before confirming that it was legitimately issued by the cluster, and a size value carried inside the identifier drives an allocation that is neither capped nor accounted for by the available memory-usage controls. The resulting out-of-memory condition is fatal and terminates the affected node process, resulting in a denial of service.	2026-08-13	6.5	CVE-2026-72687
Elastic-- Elasticsearch	A flaw in Elasticsearch allows a low-privileged authenticated user who can index documents to submit a single small document containing a crafted user-supplied input. Processing one such document occupies a worker thread from a bounded pool for a disproportionate amount of time, degrading the availability of indexing operations on the affected node.	2026-08-13	4.3	CVE-2026-72685
Elastic--Fleet Server	Authorization Bypass Through User-Controlled Key (CWE-639) in Fleet Server can lead to information disclosure via Manipulating User-Controlled Variables (CAPEC-77). The authorization decision for artifact downloads relied on a client-supplied value that was persisted without being validated against the server-side record of the requesting agent's assignment. An authenticated party in possession of a valid enrolled agent credential could therefore retrieve a policy the agent is not assigned to.	2026-08-13	6.5	CVE-2026-72657
Elastic--Fleet Server	Improper Control of Generation of Code ('Code Injection') (CWE-94) in Fleet Server can lead to the execution of attacker-supplied script content via Code Injection (CAPEC-242). Kibana accepted an identifier for an output configuration without restricting it to safe characters. That identifier is later placed into a server-side script that Fleet Server builds as part of routine agent policy processing, so script syntax embedded in the identifier became part of the script that was executed rather than being treated as data.	2026-08-13	6.5	CVE-2026-72676

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elastic--Kibana	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). A query expression accepted by a connector reporting operation was processed without any limit on its size, and an oversized expression caused the Kibana process to spend an unbounded amount of time evaluating it. An authenticated user with read-only privileges was able to send a single request that left Kibana unable to serve any user until the process was restarted.	2026-08-13	6.5	CVE-2026-49089
Elastic--Kibana	Improper Privilege Management (CWE-269) in Kibana Fleet can lead to privilege escalation via Privilege Escalation (CAPEC-233). An integration policy may optionally declare extra data streams that the integration writes to, which Fleet adds to the Elasticsearch API key issued to Elastic Agents enrolled in the corresponding agent policy. The resulting key allows new documents to be inserted and index mappings to be extended for specific indices. The key does not allow reading, updating, or deleting existing documents	2026-08-13	6.5	CVE-2026-72631
Elastic--Kibana	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated user with read-only privileges to the alerting feature could submit a specially crafted, malformed payload that causes the Kibana process to consume excessive resources. A single request is sufficient to leave Kibana unable to serve requests for all users until the process is restarted.	2026-08-13	6.5	CVE-2026-72651
Elastic--Kibana	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). An authenticated user who is authorized to manage maintenance windows could submit a specially crafted, malformed payload that causes the Kibana process to consume excessive resources. Kibana becomes unresponsive for all users and does not recover without manual intervention.	2026-08-13	6.5	CVE-2026-72653
Elastic--Kibana	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to denial of service via Excessive Allocation (CAPEC-130). A specially crafted, malformed payload submitted to a Kibana visualization feature by an authenticated user holding only low-privileged access is not correctly validated before use. Processing the request causes unbounded memory growth in the Kibana process, which is terminated by the host once available memory is exhausted. Kibana then becomes unavailable to all users until the service is restarted.	2026-08-13	6.5	CVE-2026-72659
Elastic--Kibana	Uncaught Exception (CWE-248), resulting from Improper Input Validation (CWE-20), in Kibana can lead to denial of service via Input Data Manipulation (CAPEC-153). An authenticated user holding only low-privileged access can cause an internal error condition in Kibana by supplying specially crafted data. The resulting error is raised on an execution path so it propagates as an uncaught exception and terminates the Kibana process. Kibana is unavailable to all users until the service is restarted, and the condition can be triggered repeatedly.	2026-08-13	6.5	CVE-2026-72660
Elastic--Kibana	Missing Authorization (CWE-862) in Kibana can lead to information disclosure via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). An internal Kibana data retrieval capability used by Elastic Defend endpoint response actions did not enforce the Security Solution and endpoint privileges that its user-facing equivalents require, and it retrieved data with elevated internal permissions rather than the permissions of the requesting user. As a result, an authenticated low-privileged Kibana user with no Security Solution privileges, endpoint privileges and no Elasticsearch privileges on the underlying data, could read endpoint response action records and the corresponding response content returned by managed hosts.	2026-08-13	6.5	CVE-2026-72661
Elastic--Kibana	Inefficient Algorithmic Complexity (CWE-407) in Kibana can lead to denial of service via Input Data Manipulation (CAPEC-153). A specially crafted, deeply nested expression submitted to a Kibana TSVB visualization is evaluated with a worst-case	2026-08-13	6.5	CVE-2026-72663

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cost that grows disproportionately with the size of the input. Because the evaluation runs synchronously, a single request consumes the Kibana request-processing thread indefinitely, and Kibana stops responding to all further requests until the service is restarted.			
Elastic--Kibana	Missing Authorization (CWE-862) in Kibana can lead to unauthorized execution of Elastic Defend response actions on managed hosts via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). A Kibana user who holds only detection rule authoring privileges for the Elastic Security solution can associate automated endpoint response actions with a detection rule, even though the dedicated Endpoint response action privileges that govern those capabilities (host isolation, process operations, and execute operations) have not been granted to that user. When such a rule generates alerts, the associated response actions are carried out against the matching hosts.	2026-08-13	6.5	CVE-2026-72664
Elastic--Kibana	Authorization Bypass Through User-Controlled Key (CWE-639) in Kibana can lead to unauthorized query execution against Elastic Agents that are assigned to a Kibana space the requesting user has no access to, via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). A user who is authorized to run Osquery live queries in one space can have a query carried out on hosts belonging to another space, resulting in disclosure of information from those hosts to the Osquery results data stream.	2026-08-13	6.8	CVE-2026-72666
Elastic--Kibana	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to a denial of service via Excessive Allocation (CAPEC-130). A specially crafted request submitted by an authenticated user with minimal privileges to a validation capability of the Observability log analysis feature causes Kibana to perform an unbounded amount of concurrent work. This can exhaust the memory available to the Kibana process and make Kibana unavailable to all users until it is restarted. The severity of the outcome depends on the resources allocated to the deployment; on well-provisioned deployments a single request may cause degraded performance and elevated memory pressure rather than a full outage, but the request is inexpensive to repeat.	2026-08-13	6.5	CVE-2026-72667
Elastic--Kibana	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to a denial of service via Excessive Allocation (CAPEC-130). A user-supplied list of document fields accepted by the Kibana Playground for RAG feature was neither bounded in length nor de-duplicated before it was used to assemble the response for each matching document. A single crafted request could therefore make Kibana build a response far larger than the data it was derived from, and the resulting processing and memory pressure exhausts the resources of the Kibana instance.	2026-08-13	6.5	CVE-2026-72674
Elastic--Kibana	Kibana Agent Builder A2A JSON-RPC API endpoint derives the identifier of a stored conversation from a user-supplied input, and the ownership check on that identifier does not distinguish between a conversation that does not exist and one that exists but belongs to another user. As a result, an authenticated user holding only the Agent Builder read privilege can supply an identifier already in use by another user in the same space and cause that user's conversation to be replaced and reassigned to the requesting account. The original owner permanently loses access to the conversation and its history. The impact is limited to loss of integrity and availability of the affected conversation; the attacker does not read the overwritten content.	2026-08-13	6.5	CVE-2026-72680
Elastic--Kibana	Kibana Agent Builder does not correctly verify that the requesting user holds the privileges required by a separate Kibana feature before it creates and runs a tool that invokes that feature's functionality. This allows privilege escalation and could lead to disclosure of sensitive information that the user is not authorized to read.	2026-08-13	6.5	CVE-2026-72681
Elastic--Kibana	Incorrect Authorization (CWE-863) in Kibana can lead to unauthorized deletion of Synthetics private locations via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). Synthetics private locations can be shared with more than one	2026-08-13	5.4	CVE-2026-72673

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	space, and deleting one removes it from every space it is shared with. The safeguard that prevented the deletion of a private location still in use evaluated only the monitors visible in the requesting user's own space, so monitors that depend on the private location in other spaces were not taken into account. As a result, an authenticated Kibana user holding the Synthetics write privilege in a single space could delete a private location that other spaces still depend on, even where the user has no access to those spaces. Deleting the private location removes the shared configuration and stops the monitors in the other spaces from running, which suppresses the availability monitoring those spaces rely on.			
Elastic--Kibana	Uncaught Exception (CWE-248) in Kibana Cases can lead to denial of service via Input Data Manipulation (CAPEC-153). Malformed link syntax stored in a case comment was not rejected or sanitized when the comment was later formatted for display, and the resulting unhandled error prevented the affected case from being displayed. An authenticated user holding privileges to comment on a case could store such a comment, after which that case became inaccessible to every user who opened it until the stored comment was removed.	2026-08-13	4.3	CVE-2026-49096
Elastic--Kibana	Authorization Bypass Through User-Controlled Key (CWE-639) in Kibana can lead to information disclosure via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). An authenticated user who is authorized to read alerting rules in a single Kibana space could retrieve alerting rule execution telemetry that belongs to spaces the user is not authorized to access. The disclosed telemetry includes rule identifiers, rule names, space identifiers, execution outcomes, timestamps, and execution counters.	2026-08-13	4.3	CVE-2026-72650
Elastic--Kibana	Improperly Controlled Modification of Dynamically-Determined Object Attributes (CWE-915) in the case management functionality of Elastic Security in Kibana can lead to unauthorized modification of case data by an authenticated user who has not been granted case editing privileges, via Manipulating User-Controlled Variables (CAPEC-77). Object attributes accepted by the case management API were not subject to the same authorization enforcement applied in the user interface, so a low-privileged user could alter case records they were only entitled to view.	2026-08-13	4.3	CVE-2026-72655
Elastic--Kibana	A Kibana Machine Learning capability that removes a saved object from the current space accepts machine learning trained models as a target, but it verifies only the privileges that apply to anomaly detection jobs and data frame analytics jobs. A user whose role grants create anomaly detection jobs and data frame analytics jobs without the trained model privilege can therefore remove a trained model from a space. The model itself is not deleted and remains available in its other spaces, and the change can be reversed by a suitably privileged user.	2026-08-13	4.3	CVE-2026-72671
ElkArte Forum--ElkArte	A stored cross-site scripting vulnerability in ElkArte Forum 2.0 Beta 1 allows any registered member to inject persistent JavaScript into the profile fields cust_blurb and cust_locate. The fields are saved without HTML encoding and rendered unescaped in profile views visible to administrators. An attacker can craft a payload that executes in an administrator session, enabling session hijacking or privilege escalation.	2026-08-11	5.4	CVE-2026-72553
emarket-design--Video Gallery YouTube Gallery, Playlist & Video Grid	The Youtube Showcase plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 4.0.4 via the 'emd_mb_meta' shortcode. This is due to insufficient input sanitization and output escaping on attachment titles referenced by the shortcode's image field: EMD_MB_Helper::image_info() returns the attachment's raw post_title, and EMD_MB_Helper::shortcode() interpolates it into title="%s" HTML attributes via sprintf() without esc_attr(). This makes it possible for authenticated attackers, with author-level access and above (upload_files capability required to create the attachment, edit_posts/publish_posts to embed the shortcode), to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-16	6.4	CVE-2026-15790

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
emlog--emlog	Emlog is an open source website building system. In 2.6.26 and earlier, missing CSRF protection on the AI Assistant execute_tool action in admin/ai.php lets a remote unauthenticated attacker submit a forged cross-site request from an attacker-controlled page to a recently logged-in administrator. The authentication cookie set in include/lib/loginauth.php has no explicit SameSite attribute, enabling Chrome's temporary Lax+POST grace window. The query_database case passes attacker-controlled sql and confirm_code values to Ai::queryDatabase in include/service/ai.php; read queries need no confirmation, write queries accept the public confirm string, only the blog table is write-protected, and aliasing password as pwd_hash bypasses output redaction. A successful request can read every database table and write every table except blog, including changing the user table to take over an administrator account. No fixed version is available as of this review.	2026-08-14	6.8	CVE-2026-73847
encode--django-rest-framework	Django REST framework is a toolkit for building Web APIs. Prior to 3.17.2, Django REST Framework's request.data parsing in rest_framework/request.py Request._parse() passes the underlying HttpRequest stream to JSONParser and FormParser for application/json and application/x-www-form-urlencoded bodies, bypassing Django's DATA_UPLOAD_MAX_MEMORY_SIZE protection and allowing oversized request bodies to consume additional memory and CPU. This issue is fixed in version 3.17.2.	2026-08-11	5.3	CVE-2026-73228
encode--django-rest-framework	Django REST framework is a powerful and flexible toolkit for building Web APIs. Prior to 3.17.2, Django REST Framework's rest_framework/renderers.py AdminRenderer.render() uses override_method() to simulate GET and directly invokes view.get() without view.check_permissions() while rendering an invalid write request, allowing a 400 Bad Request HTML response to disclose data from a GET representation that the requester is not permitted to access. This issue is fixed in version 3.17.2.	2026-08-11	4.3	CVE-2026-73229
EnzoVezzaro--mcp-dominican-layer	A flaw has been found in EnzoVezzaro mcp-dominican-layer up to 39dd373786712650097ad31db27d5c477c8f9c82. The affected element is the function axios.get of the file src/index.ts of the component parse-csv tool. This manipulation of the argument csvUrl causes server-side request forgery. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-13	6.3	CVE-2026-19751
EnzoVezzaro--mcp-dominican-layer	A vulnerability was found in EnzoVezzaro mcp-dominican-layer up to 39dd373786712650097ad31db27d5c477c8f9c82. This affects the function parse-pdf of the file src/index.ts of the component PDF Parsing. Performing a manipulation of the argument pdfUrl results in server-side request forgery. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-13	6.3	CVE-2026-19752
ericcornelissen--shescape	Shescape before 2.1.15 (and 3.0.0 before 3.0.2) fails to properly escape tilde (~) characters in assignment contexts on Unix systems where the shell is explicitly configured to "sh" or true and /bin/sh points to BusyBox. Using the escape and escapeAll APIs with untrusted input in an assignment prefixed to a command, an attacker can inject a tilde payload to disclose the user's home directory location and, depending on usage, alter the location on which a command operates.	2026-08-15	4.8	CVE-2026-73055
Eugeniy--russh	Russh is a Rust SSH client & server library. Prior to 0.62.4, a malicious SSH server can crash a russh client session with a malformed KEX_ECDH_REPLY containing a server ephemeral value that is not 32 bytes long. The client-side Curve25519Kex::compute_shared_secret function in russh/src/kex/curve25519.rs passes the decoded exchange.server_ephemeral value to clone_from_slice without validating its length, causing a deterministic panic before the server host key is	2026-08-12	5.3	CVE-2026-73429

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	verified. The panic terminates the spawned client session task and surfaces as a JoinError, while the embedding process normally remains running. This issue is fixed in version 0.62.4.			
Eugeniy--russh	Russh is a Rust SSH client & server library. Prior to 0.62.4, an unauthenticated SSH client can cause a denial of service by sending SSH_MSG_KEX_ECDH_INIT with a 32-byte all-zero Q_C value. Curve25519Kex::server_dh in russh/src/kex/curve25519.rs accepts the all-zero peer public value and computes an all-zero shared secret, after which compute_exchange_hash calls encode_mpint in russh/src/kex/mod.rs and indexes beyond the end of the input while skipping leading zero bytes. The resulting panic occurs before authentication and terminates the server key-exchange task. This issue is fixed in version 0.62.4.	2026-08-12	5.3	CVE-2026-73430
Eugeniy--russh	Russh is a Rust SSH client & server library. Prior to 0.62.4, an authenticated SSH client can cause a denial of service by sending a pty-req channel request with more than 130 terminal-mode records. The parser in russh/src/server/encrypted.rs stores terminal modes in a fixed 130-entry [(Pty::TTY_OP_END, 0); 130] array but continues increasing the mode count, then constructs an out-of-bounds slice and panics before the application pty_request handler runs. The panic terminates the server session task without causing memory corruption. This issue is fixed in version 0.62.4.	2026-08-13	4.3	CVE-2026-73489
expresstech--Quiz and Survey Master (QSM) Quiz Maker & Survey Maker	The Quiz and Survey Master (QSM) - Easy Quiz and Survey Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'question_title' parameter in all versions up to, and including, 11.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-16	6.4	CVE-2026-11780
expresstech--Quiz and Survey Master (QSM) Quiz Maker & Survey Maker	The Quiz and Survey Master (QSM) - Easy Quiz and Survey Maker plugin for WordPress is vulnerable to generic SQL Injection via 'randon_category' Quiz Option in all versions up to, and including, 11.2.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-16	6.5	CVE-2026-15963
extendthemes--Kubio AI Page Builder	The Kubio AI Page Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.8.5. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to overwrite front-page configuration options (show_on_front, page_on_front, and page_for_posts), rewrite primary navigation menu items, replace template parts, and overwrite the Kubio global-data post. Although a nonce check via check_ajax_referer() is present, the nonce is unconditionally emitted into window.kubioUtilsData for every user who can load the block editor, making it harvestable by any Contributor and therefore an ineffective authorization barrier.	2026-08-16	4.3	CVE-2026-16779
eyaushev--swagger-testcase-mcp	A security flaw has been discovered in eyaushev swagger-testcase-mcp 5babb27c951fb404bc2b25ec80593616e49054e5. This vulnerability affects the function loadSource of the file src/utis/swagger-parser.ts of the component fetch_swagger. Performing a manipulation results in server-side request forgery. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-14	6.3	CVE-2026-19765
faiyazalam--User Login History	The User Login History plugin for WordPress is vulnerable to SQL Injection via the 'blog_id' parameter in all versions up to, and including, 2.1.7. This is due to insufficient escaping on the user supplied parameter and lack of sufficient	2026-08-16	4.9	CVE-2026-2283

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is only exploitable on multisite installations.			
fastschema--fastschema	A stored cross-site scripting (XSS) vulnerability in fastschema through v0.15.1 allows a low-privileged authenticated user to upload an SVG file containing malicious JavaScript by bypassing the MIME type allow-list check.	2026-08-10	5.4	CVE-2026-72583
feedmob--fm-mcp-servers	A vulnerability was identified in feedmob fm-mcp-servers 0.0.3. Affected by this vulnerability is the function downloadReport of the file src/smadex-reporting/src/index.ts of the component Download Endpoint. The manipulation of the argument downloadUrl leads to server-side request forgery. The attack can only be performed from a local environment. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-14	5.3	CVE-2026-19770
fifu.app--Featured Image from URL	Contributor Cross Site Scripting (XSS) in Featured Image from URL <= 5.3.3 versions.	2026-08-13	6.5	CVE-2026-73340
filebrowser--filebrowser	filebrowser versions before v2.63.21 fail to canonicalize paths before evaluating access rules, allowing authenticated users to bypass administrator-defined deny rules using case-variant or backslash-separated paths. Attackers can request files with alternate path representations that match no rule but resolve to the same filesystem object, gaining unauthorized access to denied files within their scope.	2026-08-14	6.8	CVE-2026-72835
filebrowser--filebrowser	FileBrowser versions before 2.63.19 fail to enforce the declared Upload-Length in the TUS resumable-upload PATCH endpoint, allowing authenticated users to write arbitrary data to disk. Attackers can send oversized request bodies that exceed the declared upload length to exhaust available disk space and cause service unavailability.	2026-08-14	6.5	CVE-2026-72838
filebrowser--filebrowser	File Browser versions from 2.50.0 through 2.63.21 fail to validate JWT expiration when proxy authentication is configured with a non-default logout page. Attackers with a previously valid token can access protected routes and administrative endpoints indefinitely, and exchange expired tokens for fresh ones via the renewal endpoint.	2026-08-13	6.8	CVE-2026-73611
filebrowser--filebrowser	filebrowser before 2.63.19 contains a permission bypass in the /api/resources endpoint. The checksum (?checksum=) branch of resourceGetHandler reads the entire file to compute a digest and returns it without performing a Perm.Download check (unlike the sibling raw, preview, and subtitle paths). As a result, an authenticated user provisioned with Perm.Download=false can obtain a content-hash oracle for any same-scope file (md5/sha1/sha256/sha512), enabling confirmation of known/guessed content, change detection, and offline brute-force of low-entropy files. This is an incomplete fix of CVE-2026-35606; it bypasses only the Download permission and does not defeat scope/path authorization.	2026-08-14	4.3	CVE-2026-72834
fishpie--Image Uploader for Welcart	The Image Uploader for Welcart plugin for WordPress is vulnerable to generic SQL Injection via the 'post_title' parameter in all versions up to, and including, 1.4.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with author-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-15	6.5	CVE-2026-16080
flavorjones--loofah	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. Prior to 2.25.2, Loofah's HTML5 sanitizer applies its local-reference restriction only to the xlink:href attribute on SVG use and felImage elements, while browsers also accept the plain href attribute. A crafted sanitized SVG can therefore reference an arbitrary same-origin external document; use may render external SVG content containing scripts or other	2026-08-12	4.7	CVE-2026-73490

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	dangerous content, and felmage may load external images for tracking. Applications that sanitize user-supplied SVG with Loofah's default allowlist are affected. This issue is fixed in version 2.25.2.			
FlowiseAI--Flowise	Flowise before 3.1.3 contains an incomplete credential redaction vulnerability in the GET /api/v1/credentials/:id endpoint that returns decrypted secrets in plaintext. Authenticated users with credentials:view permission can retrieve sensitive data including database connection URLs with embedded passwords, cloud service account JSON with private keys, and API keys by calling this endpoint.	2026-08-13	6.5	CVE-2026-73604
Fortinet--FortiOS	A Stack-based Buffer Overflow vulnerability [CWE-121] vulnerability in Fortinet FortiOS 7.6.1 through 7.6.6 may allow an unauthenticated attacker who can bypass stack protection and ASLR to execute arbitrary code or commands in the context of the WAD daemon via crafted sockets, only if the explicit proxy is configured with Kerberos authentication and SOCKS enabled.	2026-08-12	5.1	CVE-2026-71407
Fortinet--FortiOS	A allocation of resources without limits or throttling vulnerability in Fortinet FortiOS 7.6.0 through 7.6.6, FortiOS 7.4 all versions, FortiOS 7.2 all versions may allow attacker to denial of service via <insert attack vector here>	2026-08-12	5	CVE-2026-71408
Fortinet--FortiWeb	A incomplete list of disallowed inputs vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.2, FortiWeb 7.6.0 through 7.6.5, FortiWeb 7.4 all versions, FortiWeb 7.2 all versions, FortiWeb 7.0 all versions may allow attacker to improper access control via <insert attack vector here>	2026-08-12	4.8	CVE-2026-70466
Foxit Software Inc.--Foxit PDF Editor	Foxit PDF Editor/Reader inconsistently alerts users when signature fields are abnormally modified, including alterations to appearance, coordinates, or field duplication. This may mislead users into trusting tampered documents, since the UI cannot accurately reflect the actual integrity status of signatures.	2026-08-13	4.7	CVE-2026-18622
francoisjacquet--RosarioSIS	A vulnerability has been found in francoisjacquet RosarioSIS up to 12.7.4. This vulnerability affects unknown code of the file modules/Students/includes/Medical.inc.php of the component Student Medical Module. Such manipulation of the argument table leads to sql injection. The attack may be launched remotely. Upgrading to version 12.8 is able to resolve this issue. The name of the patch is 6234a0ee0124c0667c824693ac77164f18946ddf. Upgrading the affected component is recommended.	2026-08-14	6.3	CVE-2026-19785
francoisjacquet--RosarioSIS	A flaw has been found in francoisjacquet RosarioSIS up to 12.8. This affects the function DBUupdate of the file Discipline/Referrals.php. This manipulation causes authorization bypass. The attack may be initiated remotely. The exploit has been published and may be used. Upgrading to version 12.9 is able to mitigate this issue. Patch name: 04dd1a368ddf80ad7082baefa3c656e4e1825c76. It is suggested to upgrade the affected component.	2026-08-14	4.3	CVE-2026-19784
francoisjacquet--RosarioSIS	A vulnerability was found in francoisjacquet RosarioSIS up to 12.8. This issue affects some unknown processing of the file Modules.php. Performing a manipulation results in cross-site request forgery. Remote exploitation of the attack is possible. Upgrading to version 12.9 is capable of addressing this issue. The patch is named 801a71272c82cf4bf695fdc5ed42a9b7511d124d. It is recommended to upgrade the affected component.	2026-08-14	4.3	CVE-2026-19786
frappe--erpnext	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.111.0 and 16.22.0, the add_ac function in erpnext/accounts/utis.py accepts the ignore_permissions argument without enforcing Account create permission, allowing an authenticated limited user to create unauthorized accounting master records and affect financial data integrity and audit trails. This issue is fixed in versions 15.111.0 and 16.22.0.	2026-08-10	6.5	CVE-2026-72907
frappe--erpnext	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.109.0 and 16.20.0, the get_tax_template function in erpnext/accounts/doctype/tax_rule/tax_rule.py constructs an SQL WHERE clause	2026-08-10	6.5	CVE-2026-72908

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	from request-influenced posting_date and args values, allowing an authenticated low-privilege user to inject SQL and extract sensitive information. This issue is fixed in versions 15.109.0 and 16.20.0.			
frappe--erpnext	ERPNext is a free and open source Enterprise Resource Planning tool. Prior to 15.111.0 and 16.22.0, the send_auto_email function in erpnext/accounts/doctype/process_statement_of_accounts/process_statement_of_accounts.py lacks a Process Statement Of Accounts permission check, allowing an authenticated low-privilege user to trigger automated emails outside the permitted role. This issue is fixed in versions 15.111.0 and 16.22.0.	2026-08-10	4.3	CVE-2026-72906
FreeCAD--FreeCAD	FreeCAD is a free and open-source multiplatform 3D parametric modeler. Prior to 1.1.2, the Xerces SAX2 XMLReader constructed in src/Base/Reader.cpp by Base::XMLReader::XMLReader() parses attacker-controlled Document.xml from a crafted .FCStd archive without disabling default external entity resolution or external DTD loading. When Document::restore() opens the document, external entities can read local files through the file URI scheme or initiate server-side requests through the http URI scheme, and resolved content can flow through the characters() callback. This issue is fixed in version 1.1.2.	2026-08-11	6.1	CVE-2026-73235
Friendica--Friendica	A server-side request forgery vulnerability in Friendica through the 2026.08-dev branch allows authenticated users with a free self-registered account to probe internal network services via the link-preview endpoint. The endpoint fetches any user-supplied URL without applying an internal IP deny list. An attacker can use this to scan the internal network or access cloud metadata services.	2026-08-11	6.5	CVE-2026-72597
Froiden--Worksuite SaaS	Worksuite SaaS versions prior to 6.0.14 contains a stored cross-site scripting vulnerability in the Asset Management module that allows authenticated administrators to inject arbitrary JavaScript by entering malicious payloads into the Location and Description fields when creating a new asset. Attackers can store crafted HTML script tags in the application database that execute automatically in the browsers of any user who views the affected asset, potentially leading to session hijacking, credential theft, and unauthorized actions on behalf of authenticated users.	2026-08-13	4.8	CVE-2026-18741
gchq--CyberChef	CyberChef is a web app for encryption, encoding, compression, and data analysis. Prior to 11.3.0, CyberChef's pretty-recipe parser in src/core/Utils.mjs can exhaust client-side CPU when a malformed #recipe= URL fragment containing a large number of unmatched quote characters reaches Utils.parseRecipeConfig(). The function synchronously applies a complex global regular expression that may perform heavy backtracking before rejecting the input, causing the victim's browser tab to freeze during startup for seconds or longer. No code execution, data exfiltration, or privilege escalation occurs. This issue is fixed in version 11.3.0.	2026-08-10	4.3	CVE-2026-72912
getgrav--grav	Grav Form plugin versions before 9.1.15 contain a stored cross-site scripting vulnerability in radio and toggle field option labels rendered with the Twig raw filter. Attackers with form authoring permissions can inject HTML and script payloads in option labels that execute in the browsers of visitors and administrators viewing the form.	2026-08-14	5.4	CVE-2026-72821
getgrav--grav	The Grav API plugin (getgrav/grav-plugin-api) before 1.0.13 contains an API-key scope cap bypass in DemoController. Its private requireSuper() method checks isSuperAdmin() and returns early before invoking requirePermission(), so the api_key_scopes cap (enforced only in requirePermission()) is skipped. As a result, any scoped API key minted on a super account can bypass its scope restrictions when calling the baseline() and reset() operations (e.g. POST /api/v1/demo/reset), allowing it to capture the demo baseline or force a demo reset. Impact is bounded to demo-engine control and is conditional on demo mode being configured with writable resources.	2026-08-14	5.4	CVE-2026-72823

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getgrav--grav	Grav versions from 1.5.2 through 2.0.12 contain a stored cross-site scripting vulnerability in the Security::detectXss() function (system/src/Grav/Common/Security.php). The event-handler scan is anchored at '<' and uses '[^>]*?', which cannot cross the first literal '>'; when a '>' appears inside a quoted attribute value the browser keeps the tag open and parses a subsequent event handler (e.g. onerror), so the detector and browser disagree. A page editor without admin.super privileges can save page content such as '" onerror=alert(document.domain)>', which is accepted, stored, and executed in the site origin when any visitor (including unauthenticated users) views the page. Fixed in 2.0.13.	2026-08-14	5.4	CVE-2026-72832
getgrav--grav	Grav versions before 2.0.13 fail to properly validate backup profile root paths, allowing attackers to archive directories outside GRAV_ROOT when not in the hard-coded deny-list. Attackers with profile editor access can configure backup profiles with traversal paths to expose sensitive files from locations like /opt, /mnt, or /srv.	2026-08-14	4.9	CVE-2026-72820
getprobo--probo	Probo is a self-hostable governance, risk, and compliance (GRC) platform built for engineering and security teams. Probo's `saferedirect` package validates redirect URLs used across authentication flows (OIDC, SAML, session transfer, OAuth connectors, and trust-center magic links). Prior to version 0.19.3.1, the validator only inspected the second character of relative paths, so a URL like `./../evil.com` passed validation because the second character is `.`. Go's `http.Redirect` normalizes this path to `../evil.com` before setting the `Location` header. Browsers can interpret the backslash as a host separator and redirect the user to an external domain (`https://evil.com`), bypassing the intended same-origin restriction. This enables open-redirect phishing: an attacker can craft a `continue` parameter (or embed a malicious URL in a session-transfer token) that appears to originate from a trusted Probo domain but redirects victims elsewhere. This is fixed in `go.probo.inc/probo` 0.193.1 by normalizing relative paths with `path.Clean` before validation, rejecting backslashes (including percent-encoded `%5c`) anywhere in the path, and re-checking the normalized result for protocol-relative and backslash prefixes. Self-hosted deployments should upgrade to probod v0.194.1 or later. SaaS deployments on getprobo.com are patched. No practical workaround is available for self-hosted installations.	2026-08-13	4.7	CVE-2026-49820
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.5 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed an unauthenticated user to cause a denial of service due to improper input validation.	2026-08-12	5.3	CVE-2026-7427
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 17.7 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user to view restricted configuration settings due to improper authorization checks on a group settings page.	2026-08-12	4.3	CVE-2026-18244
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.4 and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user to read policy configuration belonging to a namespace they were not authorized to access, due to incorrect authorization checks in a GraphQL query.	2026-08-12	4.3	CVE-2026-18433
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 16.0 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user with developer-role permissions to view external status check configuration restricted to higher-privileged roles due to missing authorization on a merge request API endpoint.	2026-08-12	4.3	CVE-2026-4879
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 12.0 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user to bypass IP-based access restrictions	2026-08-12	4.3	CVE-2026-6821

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and read limited merge request information from a private project due to missing authorization checks in a merge requests API endpoint.			
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.6 before 19.0.6, 19.1 before 19.1.4, and 19.2 before 19.2.2 that under certain conditions could have allowed an authenticated user with developer role to modify certain package registry metadata without the required maintainer-level permissions due to improper authorization checks.	2026-08-12	4.3	CVE-2026-8667
gitpython-developers--GitPython	GitPython before 3.1.57 contains an incomplete denylist in the <code>unsafe_git_archive_options</code> guard that omits <code>--add-file</code> and <code>--add-virtual-file</code> options. Attackers can supply these options to <code>Repo.archive()</code> to read arbitrary files from the filesystem and include them in the returned archive.	2026-08-13	6.5	CVE-2026-73619
gitpython-developers--GitPython	GitPython before 3.1.56 contains an argument injection vulnerability in the <code>Commit.count()</code> method, which forwards keyword arguments to 'git rev-list' without the <code>check_unsafe_options</code> guard present in the sibling <code>iter_items</code> method. An attacker who can control options passed to <code>Commit.count</code> (e.g., via an application that forwards a user-supplied options dict) can supply <code>output=<path></code> , causing 'git rev-list --output=<path>' to open and truncate the target file to zero bytes before revision parsing. This allows destruction/blinking of an arbitrary file at the process's privilege level (no content control, 0-byte truncation).	2026-08-13	5.4	CVE-2026-73621
go-chi--chi	go-chi/chi through 5.2.1 contains an IP spoofing vulnerability in the RealIP middleware (<code>middleware/realip.go</code>). The <code>realIP()</code> function reads client-controlled headers (<code>True-Client-IP</code> , <code>X-Real-IP</code> , and <code>X-Forwarded-For</code>) and overwrites <code>r.RemoteAddr</code> without verifying that the request originated from a trusted proxy. Attackers can supply arbitrary IP addresses in these headers to bypass IP-based access controls, evade rate limiting and geo-IP restrictions, and pollute audit logs. Fixed in 5.3.0.	2026-08-14	6.5	CVE-2026-72816
go-chi--chi	go-chi/chi versions 0.9.0 before 5.3.0 contains an IP spoofing vulnerability in the RealIP middleware, which resolves the request source IP (<code>Request.RemoteAddr</code>) using the first IP in the <code>X-Forwarded-For</code> header without validating trusted proxies. A malicious client can prepend a forged IP as the first value of the <code>X-Forwarded-For</code> header to spoof the request source IP, potentially bypassing access controls or falsifying request logs.	2026-08-14	6.5	CVE-2026-72817
gomarble-ai--facebook-ads-mcp-server	A vulnerability has been found in gomarble-ai facebook-ads-mcp-server 0.1.0. The impacted element is the function <code>fetch_pagination_url</code> of the <code>file_server.py</code> . Such manipulation leads to server-side request forgery. The attack can be launched remotely. The name of the patch is <code>4e53875aa22e8991c2fa4a7660d86e1caba66659</code> . Applying a patch is advised to resolve this issue.	2026-08-16	6.3	CVE-2026-19956
Grafana Labs--Grafana	An authorization bypass vulnerability in Grafana through 13.2.0 allows an Editor-role user to delete protected contact points (receivers) without the required <code>alert.notifications.receivers.protected:write</code> permission.	2026-08-10	6.5	CVE-2026-72585
graphlit--graphlit-mcp-server	A vulnerability was identified in graphlit graphlit-mcp-server 1.0.1. This affects the function <code>fetch</code> of the file <code>src/tools.ts</code> of the component <code>ssrf-test</code> Endpoint. Such manipulation of the argument <code>url</code> leads to server-side request forgery. The attack may be launched remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-16	6.3	CVE-2026-19957
Grokability--Snipe-IT	Snipe-IT before 8.6.0 contains an authorization bypass (insecure direct object reference) in the <code>asset checkout-request cancellation</code> endpoint. The <code>cancel_by_admin</code> and <code>requestingUser</code> values are read from user-controlled URL path segments and used without a server-side authorization check, so any authenticated, low-privileged user can supply a non-empty <code>cancel_by_admin</code> value to bypass the request-ownership check and cancel another user's pending	2026-08-11	5.4	CVE-2026-19579

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	checkout request. Because asset and user identifiers are sequential integers, an attacker can enumerate them to cancel every pending checkout request, disrupting the asset-request workflow. This is fixed in Snipe-IT 8.6.0.			
GStreamer--gst-plugins-good	A flaw was found in GStreamer gst-plugins-good (avidemux). When parsing FUJIFILM metadata in an AVI strd chunk, gst_avi_demux_parse_strd() decrements a remaining-length counter by fixed offsets (98 and 10 bytes) without verifying sufficient data remains. For crafted strd payloads of exactly 106 or 107 bytes, the counter underflows to a very large unsigned value, causing subsequent null-terminated string scanning to read far beyond the allocated heap buffer. Date-format normalization may also write beyond the buffer end. Confirmed impacts include heap out-of-bounds read, out-of-bounds write, heap information disclosure (adjacent data appearing in parsed metadata), and application crash/denial of service. The avidemux element is auto-plugged by playbin, decodebin, and gst-discoverer, so opening or previewing a crafted AVI is sufficient to trigger the issue. Fixed upstream in gst-plugins-good 1.28.6 (GStreamer-SA-2026-0072).	2026-08-12	6.6	CVE-2026-73433
GStreamer--gst-plugins-good	A flaw was found in GStreamer gst-plugins-good (avidemux). In gst_avi_demux_riff_parse_vprp(), the number of available gst_riff_vprp_video_field_desc entries is calculated by dividing the remaining buffer size by the attacker-controlled vprp->fields value, rather than by sizeof(gst_riff_vprp_video_field_desc). This can cause the parser to treat more field descriptors as available than fit in the input buffer, resulting in out-of-bounds reads. Processing a crafted AVI via playbin/decodebin can crash the application (denial of service). Fixed upstream in gst-plugins-good 1.28.6 (GStreamer-SA-2026-0072).	2026-08-12	6.1	CVE-2026-73434
HashiCorp--Vault	Vault's ACL policy engine did not consistently enforce a wildcard (glob) deny rule against LIST requests made with a trailing slash on the denied path. This may allow a token holding a broader allow rule alongside a narrower wildcard deny rule to enumerate the names of entries beneath a path it was intended to be denied access to. This vulnerability (CVE-2026-12624) is fixed in Vault Community Edition 2.0.3 and Vault Enterprise 2.0.3, 1.21.8, 1.20.13, and 1.19.19.	2026-08-10	4.3	CVE-2026-12624
HCL Software--AION	HCL AION is affected by a vulnerability where certain endpoints lack sufficient anti-automation controls. Automated or scripted requests may be submitted without adequate rate limiting or challenge mechanisms, potentially resulting in unintended behavior or security impact under certain conditions.	2026-08-13	5.6	CVE-2025-62314
HCL Software--AION	HCL AION is affected by a vulnerability where the shared storage used by product components is architected without sufficient access separation. Processes sharing the storage may be able to access or modify files beyond their intended scope, potentially resulting in unintended behavior or security impact under certain conditions.	2026-08-13	4.7	CVE-2025-52640
HCL Software--AION	HCL AION is affected by a vulnerability where indirect prompt injection can lead to HTML injection in rendered output. Injected markup may be displayed to users, potentially resulting in unintended behavior or security impact under certain conditions.	2026-08-13	4.3	CVE-2026-21832
HCLSoftware--HCL BigFix Mobile	HCL BigFix Mobile is vulnerable to Reflected Cross-Site Scripting (Reflected XSS) due to insufficient validation and output encoding of user-controlled input.	2026-08-10	5.4	CVE-2026-56619
HCLSoftware--HCL BigFix Mobile	HCL BigFix Mobile is vulnerable to information disclosure due to improper handling of exceptions and verbose error reporting.	2026-08-10	4.3	CVE-2026-56620
honojs--node-server	@hono/node-server allows running the Hono application on Node.js. From 2.0.0 until 2.0.10, a WebSocket upgrade request to an upgradeWebSocket route with a missing or malformed Sec-WebSocket-Key header causes src/websocket.ts to retain the request's IncomingMessage in waiterMap and leave waitForWebSocket pending because ws.handleUpgrade emits no connection event. The aborted	2026-08-13	5.3	CVE-2026-73565

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	handshake therefore has no cleanup path, allowing an unauthenticated attacker to flood a public route, cause unbounded memory growth, and eventually make the service unavailable. This issue is fixed in version 2.0.10.			
HumanSignal--Label Studio	A server-side request forgery vulnerability in HumanSignal Label Studio through 1.24.0.dev0 exists because SSRF_PROTECTION_ENABLED is set to false by default. The import-from-URL endpoint fetches any caller-supplied URL including internal loopback addresses on the default installation. An authenticated user can use this to reach internal services, cloud metadata endpoints, and other resources not intended for external access.	2026-08-11	6.5	CVE-2026-72560
iatsiuk--pptr-mcp	A security flaw has been discovered in iatsiuk pptr-mcp up to 0.2.7. The impacted element is the function executeCode of the file src/vm-executor.ts of the component execute Tool. The manipulation results in code injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-16	6.3	CVE-2026-19958
IBM--DataPower Gateway 11.0.0	IBM DataPower Gateway 11.0.0.0 through 11.0.0.1 and IBM DataPower Gateway 10.5.0.0 through 10.5.0.21 and IBM DataPower Gateway 10.6.0.0 through 10.6.0.9 allows a race condition that results in improper isolation of request state when handling the built'in X'Client'IP header. Under concurrent request processing, XClient 'IP values may be contaminated across requests, enabling IP spoofing and disclosure of other clients' IP addresses.	2026-08-12	4.2	CVE-2026-7366
IBM--Db2	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.5 for Linux, UNIX and Windows (includes DB2 Connect Server) could allow a local attacker to obtain sensitive information due to the logging of plain text passwords in trace files.	2026-08-12	5.5	CVE-2026-18097
IBM--Db2	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.5 is affected by an improper authorization vulnerability in the certain command, allowing a non-privileged user to bypass authority checks and modify database catalog data.	2026-08-12	4.3	CVE-2026-16480
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to bypass security restrictions due to the ability to disable server-side input validation via a request parameter.	2026-08-14	6.3	CVE-2026-17079
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to obtain sensitive information due to improper validation of file paths.	2026-08-14	6.5	CVE-2026-17173
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to execute arbitrary scripts due to cross-site scripting.	2026-08-14	6.3	CVE-2026-17209
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to obtain sensitive information due to improper authentication.	2026-08-14	5.3	CVE-2026-16905
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to bypass security restrictions due to improper neutralization of special elements used in an SQL command.	2026-08-14	5.4	CVE-2026-17227
IBM--Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote authenticated attacker to delete arbitrary files due to path traversal.	2026-08-14	5.4	CVE-2026-18178
IBM--Documentation Offline	IBM Documentation Offline 1.0.0 through 1.4.1 could allow a remote attacker to forge valid session tokens due to the use of a hardcoded cryptographic key.	2026-08-13	5.3	CVE-2026-17468
IBM--Documentation Offline	IBM Documentation Offline 1.0.0 through 1.4.1 IBM Documentation could allow a remote attacker to obtain sensitive information due to a security misconfiguration where the documentation server binds to an unrestricted IP address.	2026-08-13	4.3	CVE-2026-16713

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to cause a denial of service due to a stack-based buffer overflow.	2026-08-13	6.5	CVE-2026-16692
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-08-12	6.4	CVE-2026-16694
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to obtain sensitive information due to an out-of-bounds read.	2026-08-13	6.5	CVE-2026-16853
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to obtain sensitive information and perform unauthorized operations due to improper validation of authentication tokens.	2026-08-13	6.5	CVE-2026-17075
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to improper limitation of a pathname to a restricted directory.	2026-08-12	6.5	CVE-2026-17266
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to bypass security restrictions due to improper validation of a session token.	2026-08-12	6.8	CVE-2026-17268
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to modify SQL tables due to improper neutralization of special elements used in an SQL command.	2026-08-12	6.5	CVE-2026-17419
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to bypass security restrictions due to improper neutralization of special elements in an SQL parameter.	2026-08-12	6.3	CVE-2026-17420
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information and bypass security restrictions due to a race condition.	2026-08-12	6.3	CVE-2026-18250
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow an authenticated attacker to force a NetServer server thread exception, caused by an integer overflow during bounds checking in request processing. The attacker could exploit this vulnerability to cause a temporary denial of service.	2026-08-13	6.5	CVE-2026-18671
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to improper processing of XML external entities.	2026-08-13	6.5	CVE-2026-18715
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to obtain sensitive information due to an out-of-bounds read.	2026-08-13	5.3	CVE-2026-16859
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to an out-of-bounds read.	2026-08-13	5.3	CVE-2026-16861
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to an out-of-bounds read.	2026-08-13	5.4	CVE-2026-16878
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to a buffer overflow.	2026-08-13	5.3	CVE-2026-16929
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to improper processing of DRDA and DDM resynchronization requests.	2026-08-13	5.3	CVE-2026-17076
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to the use of an uninitialized variable.	2026-08-13	5.3	CVE-2026-17077
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to resource exhaustion.	2026-08-13	5.3	CVE-2026-17078

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to an out-of-bounds read.	2026-08-13	5.3	CVE-2026-17212
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to an integer error when processing DRDA large-object headers.	2026-08-13	5.3	CVE-2026-17216
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information or cause a denial of service due to an out-of-bounds read.	2026-08-13	5.4	CVE-2026-17226
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to obtain sensitive information due to an out-of-bounds read.	2026-08-13	5.3	CVE-2026-17649
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to an off-by-one error in bounds checking.	2026-08-13	5.3	CVE-2026-18020
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to a heap buffer overflow.	2026-08-13	4.3	CVE-2026-16871
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to a path traversal vulnerability.	2026-08-13	4.3	CVE-2026-17088
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information and manipulate files due to a path traversal vulnerability.	2026-08-12	4.3	CVE-2026-17094
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to add unexpected parameters to a command due to parameter injection.	2026-08-12	4.3	CVE-2026-17109
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to modify data in certain SQL tables due to improper neutralization of special elements used in an SQL command.	2026-08-12	4.3	CVE-2026-17222
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to obtain sensitive information or modify data due to improper privilege management.	2026-08-13	4.4	CVE-2026-17438
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to cause a denial of service due to an improper buffer write.	2026-08-13	4.8	CVE-2026-17476
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote attacker to obtain sensitive information due to a byte-count and element-count confusion.	2026-08-13	4.3	CVE-2026-18068
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a local attacker to execute arbitrary code or cause a denial of service due to improper bounds checking.	2026-08-13	4.5	CVE-2026-18086
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to improper validation of user-supplied path input.	2026-08-12	4.3	CVE-2026-18106
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to bypass security restrictions due to improper authorization.	2026-08-12	4.3	CVE-2026-18144
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to inject arbitrary content into Navigator log files due to improper output neutralization for logs.	2026-08-12	4.3	CVE-2026-18148
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to obtain sensitive information due to a race condition.	2026-08-12	4.3	CVE-2026-18150
IBM--Security Verify Access	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 and IBM Verify Identity Access Container 11.0 through 11.0.3 Reverse Proxy in certain configurations may provide weaker than expected cryptographic validation of user supplied data.	2026-08-12	6.8	CVE-2026-17616
IBM--Security Verify Access	IBM Security Verify Access 10.0 through 10.0.9.2 and IBM Verify Identity Access 11.0 through 11.0.3 and IBM Verify Identity Access Container 11.0 through 11.0.3 is vulnerable to a denial of service attack.	2026-08-12	5.3	CVE-2026-11932

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--WebSphere Application Server - Liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is affected by a denial of service caused by insecure deserialization. A low-privileged, administrative user could exploit this vulnerability to consume system resources when the restConnector-2.0 feature is enabled.	2026-08-13	5.7	CVE-2026-10571
InstaWP--InstaWP Connect	Unauthenticated Broken Access Control in InstaWP Connect <= 0.1.3.7 versions.	2026-08-13	5.3	CVE-2026-73401
Intelliants--Subrion CMS	A path traversal vulnerability in Intelliants Subrion CMS through 4.2.1 allows authenticated administrators to delete arbitrary files on the server via the admin panel file deletion endpoint. The endpoint passes a user-supplied file path directly to unlink() without sanitization or path canonicalization. An authenticated administrator can delete sensitive system files outside the web root, potentially causing server instability or facilitating further attacks.	2026-08-11	6.5	CVE-2026-72604
qiconicdesign--KiviCare Clinic & Patient Management System (EHR)	The KiviCare - Clinic & Patient Management System (EHR) plugin for WordPress is vulnerable to generic SQL Injection via the 'searchTerm' parameter in all versions up to, and including, 4.5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires a KiviCare custom role with the 'settings_view' permission (e.g., Doctor or Receptionist), meaning standard WordPress subscribers cannot exploit this without a KiviCare-assigned role.	2026-08-15	6.5	CVE-2026-15453
itsourcecode--Hospital Management System	A weakness has been identified in itsourcecode Hospital Management System 1.0. This issue affects some unknown processing of the file viewdoctortimings.php. Executing a manipulation of the argument delid can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2026-08-14	6.3	CVE-2026-19767
itsourcecode--Hospital Management System	A security flaw has been discovered in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /viewmedicine.php. Performing a manipulation of the argument delid results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	2026-08-15	6.3	CVE-2026-19894
itsourcecode--Hospital Management System	A vulnerability has been found in itsourcecode Hospital Management System 1.0. This impacts an unknown function of the file /vieworder.php. The manipulation of the argument delid leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2026-08-16	6.3	CVE-2026-19934
JanDeDobbeleer--oh-my-posh	Oh My Posh is the most customisable and low-latency cross platform/shell prompt renderer. Prior to 29.35.1, write(s rune) in src/terminal/writer.go emitted attacker-controlled current directory names and Git metadata, including Commit.Subject, Commit.Author.Name, Commit.Author.Email, and RawUpstreamURL, without removing C0/C1 terminal control characters such as ESC, BEL, CSI, and OSC, allowing terminal escape sequence injection during prompt rendering that could overwrite the clipboard, spoof the prompt or screen, manipulate the window title, or disrupt the terminal. This issue is fixed in version 29.35.1.	2026-08-13	6.1	CVE-2026-73506
Jazzband--tablib	tablib prior to 3.10.0 contains a stored cross-site scripting vulnerability in the HTML export functionality that allows attackers to execute arbitrary JavaScript by embedding malicious payloads in dataset titles, which are interpolated unsanitized into HTML output via the export_book method in the _html.py format handler. Attackers can rename worksheet sheets in imported files such as XLSX, ODS, XLS, or YAML with script payloads that are assigned to the Dataset title attribute and rendered unescaped inside an HTML h3 tag, leading to session hijacking, unauthorized administrative actions, and sensitive data exposure when the output is rendered in a browser.	2026-08-12	5.4	CVE-2026-9318

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jfrog--artifactory	Under specific self-hosted Helm configurations, generated TLS private keys may be retained in rendered manifests accessible to highly privileged local users.	2026-08-12	6.7	CVE-2026-66016
jfrog--artifactory	A repository publisher without delete permission may modify protected package content under specific conditions.	2026-08-12	6.5	CVE-2026-68754
jfrog--artifactory	A party with write access to stored session data may affect JFrog Artifactory under specific conditions.	2026-08-12	6.6	CVE-2026-68756
jfrog--artifactory	A low-privileged authenticated user may access restricted support information under specific conditions.	2026-08-12	6.5	CVE-2026-68758
jfrog--artifactory	An unauthenticated user may access restricted repository information under specific conditions.	2026-08-12	5.3	CVE-2026-66377
jfrog--artifactory	A repository reader with cache-deploy permission may access content outside a configured upstream path under specific conditions.	2026-08-12	5.3	CVE-2026-66381
jfrog--artifactory	An authenticated user may write data outside the intended Docker cache path under specific remote-repository conditions.	2026-08-12	5.3	CVE-2026-66384
jfrog--artifactory	An unauthenticated user may access restricted Artifactory content when a credentialed remote repository is configured in a specific way.	2026-08-12	5.3	CVE-2026-68753
jfrog--artifactory	An unauthenticated user may bypass authentication under specific cache conditions.	2026-08-12	5.3	CVE-2026-68760
jfrog--artifactory	An unauthenticated user may access restricted artifacts in JFrog Artifactory under specific conditions.	2026-08-12	5.9	CVE-2026-69107
jfrog--artifactory	Credentials for a deleted user may remain valid for a short period under specific conditions.	2026-08-12	4.2	CVE-2026-66376
jfrog--artifactory	An authenticated user without repository read permission may access private NuGet metadata under specific conditions.	2026-08-12	4.3	CVE-2026-66378
jfrog--artifactory	An authenticated user may view private Puppet module metadata without repository read access.	2026-08-12	4.3	CVE-2026-66379
jfrog--artifactory	An authenticated user without repository read permission may access private OCI referrer metadata under specific conditions.	2026-08-12	4.3	CVE-2026-66380
jfrog--artifactory	An authenticated user may write files outside the intended Artifactory work directory under specific conditions.	2026-08-12	4.3	CVE-2026-66382
jfrog--artifactory	A bundle writer may create misleading release promotion information under specific conditions.	2026-08-12	4.3	CVE-2026-68755
jfrog--artifactory	An authenticated user without repository read permission may access package metadata under specific conditions.	2026-08-12	4.3	CVE-2026-70547
Jij-Inc--Jij-MCP-Server	A vulnerability was found in Jij-Inc Jij-MCP-Server 0.1.0. This affects the function PythonREPL.run of the file jij_mcp/python_repr.py of the component jm_check. The manipulation of the argument code results in code injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-16	5.5	CVE-2026-19964
kekingcn--kkFileView	kkFileView is a universal file online preview project based on Spring Boot. Prior to 5.0.1, the unauthenticated GET /addTask endpoint in kkFileView is omitted from TrustHostFilter and TrustDirFilter in server/src/main/java/cn/keking/config/WebConfig.java, allowing FileConvertQueueTask to fetch an attacker-selected URL after	2026-08-11	5.8	CVE-2026-73243

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	FileHandlerService#getFileAttribute uses the fullfilename parameter to force an OFFICE, COMPRESS, or CAD type. This issue is fixed in version 5.0.1.			
kekingcn-- kkFileView	kkFileView is a universal file online preview project based on Spring Boot. Prior to 5.0.1, the unauthenticated POST /listFiles endpoint in server/src/main/java/cn/keking/web/controller/FileController.java passes the user-controlled path parameter from FileController#getFiles to Files.newDirectoryStream without confinement to the demo directory, allowing directory enumeration outside the intended root. This issue is fixed in version 5.0.1.	2026-08-11	5.3	CVE-2026-73244
kendysond-- Payment Forms for Paystack	Subscriber Sensitive Data Exposure in Payment Forms for Paystack <= 4.0.5 versions.	2026-08-13	6.5	CVE-2026-66444
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 2.0.0-rc6, Kestra's cli/src/main/resources/application.yml serves Micronaut management endpoints on port 8081 without authentication even when Basic Auth protects /api/v1/** on port 8080, allowing unauthenticated GET /env requests to disclose resolved configuration and POST /loggers/{name} requests to change runtime log levels. This issue is fixed in 2.0.0-rc6.	2026-08-11	6.5	CVE-2026-73245
Kirki--Kirki	The Kirki WordPress plugin before 6.2.1 does not properly authorise its front-end form submission REST routes and passes attacker-controlled input through shortcode execution, allowing unauthenticated users to run any shortcode registered on the site, which on a default install leads to disclosure of the site administrator's email address and an arbitrary-recipient mail relay from the victim's domain.	2026-08-12	6.5	CVE-2026-16747
kodezen-- StoreEngine Complete eCommerce Solution with Memberships, Licensing, Affiliates & More	The StoreEngine - Complete eCommerce Solution with Memberships, Licensing, Affiliates & More plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.1.1 via the parse_file_path function. This makes it possible for authenticated attackers, with vendor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	2026-08-16	6.5	CVE-2026-15056
Koha Community-- Koha	A stored SQL injection vulnerability in Koha through 24.11.17, 25.05.12, 25.11.06, and 26.05.01 allows authenticated staff with the tools => label_creator permission to execute arbitrary SQL via the image_name field of a patron card layout. The image_name value is stored verbatim in the layout XML and later concatenated raw into a SQL query in patroncards/create-pdf.pl when a patron card batch is printed. An attacker can read the entire Koha database including patron PII and staff bcrypt password hashes via error-based or time-based blind injection.	2026-08-11	6.5	CVE-2026-72608
Koha Community-- Koha	A stored SQL injection vulnerability in Koha through 24.11.17, 25.05.12, 25.11.06, and 26.05.01 allows authenticated staff with the borrowers => edit_borrowers permission to cause a time-based denial of service by storing a SQL payload in a patron lang field. The value is concatenated raw into a subquery in Koha::AdditionalContents->search_for_display when an issue slip is printed for the affected patron. The 25-character column length limits exploitation to timing attacks; data extraction is not practical. The stored payload executes on each subsequent issue-slip print, scaling linearly with the SLEEP value and the number of slip-news rows.	2026-08-11	4.3	CVE-2026-72610
ladela--Online Scheduling and Appointment Booking System Bookly	The Bookly plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 27.7 via the appointment() method of the Mobile Staff Cabinet API (resource=appointment, action=bookly_mobile_staff_cabinet) in frontend/modules/mobile_staff_cabinet/api/handlers/Handler1_0.php. This is due to the handler loading an Appointment by the attacker-supplied params[id]	2026-08-16	4.3	CVE-2026-12905

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	without verifying that the appointment's staff_id matches the authenticated staff member, whereas sibling operations (deleteAppointment, saveAppointment, appointments list) correctly scope to \$this->staff->getId() when \$this->role === ROLE_STAFF. This makes it possible for authenticated attackers, with staff-level mobile cabinet access (any valid access_key token bound to a Staff entity), to read appointment details - including the internal note and the full customer_appointments collection (customer full_name, email, phone, notes, custom_fields, extras, payment_total, payment_type, payment_status) - belonging to other staff members by enumerating sequential appointment IDs.			
Ladybird Web Solution--Faveo Helpdesk	A broken access control vulnerability in Ladybird Web Solution Faveo Helpdesk 2.0.3 allows any self-registered customer to read ticket conversations belonging to other customers via the v1 REST API. The API verifies the existence of the requested ticket but not ownership, enabling any authenticated user to access arbitrary ticket threads including internal agent notes containing sensitive information.	2026-08-11	6.5	CVE-2026-72554
Lasso Analytics, Inc.--Do Lasso	Unauthenticated Insecure Direct Object References (IDOR) in Do Lasso <= 358 versions.	2026-08-13	6.5	CVE-2026-28155
Lenovo--E16 Gen 2 (Type 21M5, 21M6) Laptops (ThinkPad) ELAN TrackPoint Device Driver for Windows 11 (Version 23H2 or later) - ThinkPad	ELAN reported a potential out-of-bounds write vulnerability in the ELAN TrackPoint driver that, under certain circumstances, could allow a local authenticated user to cause a system crash.	2026-08-13	4.7	CVE-2026-14256
libexpat project--libexpat	libexpat before 2.8.3 has an out-of-bounds read and resultant infinite loop because low surrogates are treated the same as high surrogates during Unicode processing in the *_toUtf16 functions.	2026-08-10	6.2	CVE-2026-72522
magepeopleteam--WpBookingly	Customer Cross Site Scripting (XSS) in WpBookingly <= 1.3.2 versions.	2026-08-13	6.5	CVE-2026-66687
Maruti Mohanty--WP Social Avatar	Unauthenticated Broken Access Control in WP Social Avatar <= 1.5 versions.	2026-08-13	6.5	CVE-2026-66454
Mattermost--Mattermost	Mattermost versions 11.9.x <= 11.9.0, 11.8.x <= 11.8.4, 11.7.x <= 11.7.7, 10.11.x <= 10.11.22 fail to properly limit resource consumption when processing certain user-supplied input, which allows an authenticated user to cause a denial of service. Mattermost Advisory ID: MMSA-2026-00713	2026-08-13	6.5	CVE-2026-14298
matthiasnordwig--Invisible Anti-Spam & CAPTCHA reCAPTCHA Alternative for All Forms	The Invisible Anti-Spam & CAPTCHA - reCAPTCHA Alternative for All Forms plugin for WordPress is vulnerable to generic SQL Injection via the 'key' parameter in all versions up to, and including, 5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with editor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-15	4.9	CVE-2026-16094
matthiasnordwig--Invisible Anti-Spam & CAPTCHA reCAPTCHA Alternative for All Forms	The Invisible Anti-Spam & CAPTCHA - reCAPTCHA Alternative for All Forms plugin for WordPress is vulnerable to generic SQL Injection via Pattern JSON Keys/Values in all versions up to, and including, 5.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with editor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-15	4.9	CVE-2026-16146

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Metabase--Metabase	Metabase allows an authenticated, low-privileged attacker to read the entire Metabase application database.	2026-08-10	6.5	CVE-2026-72900
Microsoft--.NET 10.0	Inconsistent interpretation of http requests ('http request/response smuggling') in .NET allows an unauthorized attacker to bypass a security feature over a network.	2026-08-11	5.9	CVE-2026-62899
Microsoft--.NET 10.0	Improper removal of sensitive information before storage or transfer in .NET allows an unauthorized attacker to disclose information over a network.	2026-08-11	5.9	CVE-2026-62900
Microsoft--.NET 8.0	Inclusion of functionality from untrusted control sphere in .NET allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-62902
Microsoft--Azure CycleCloud 8.9.2	Missing authorization in Azure CycleCloud allows an authorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-65806
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-70327
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-70328
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62842
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-63517
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-63521
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-63524
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-63528
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-63529
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-63530
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-63531
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-64899
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-64917

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft 365 Apps for Enterprise	Off-by-one error in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-66806
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-66809
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-66810
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-68797
Microsoft-- Microsoft 365 Apps for Enterprise	Use of uninitialized resource in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-68799
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-68802
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-68808
Microsoft-- Microsoft 365 Apps for Enterprise	Incomplete cleanup in Microsoft Office PowerPoint allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-68809
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-68813
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70310
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office PowerPoint allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70312
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70314
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70315
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office PowerPoint allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70316
Microsoft-- Microsoft 365 Apps for Enterprise	Use of uninitialized resource in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70317
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70318

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70319
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office PowerPoint allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70320
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office PowerPoint allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70322
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70323
Microsoft-- Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office PowerPoint allows an unauthorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-70325
Microsoft-- Microsoft 365 Apps for Enterprise	Insufficiently protected credentials in Microsoft Office Outlook allows an unauthorized attacker to perform spoofing over a network.	2026-08-11	4.3	CVE-2026-62882
Microsoft-- Microsoft Defender for Endpoint for Mac	Exposure of sensitive information to an unauthorized actor in Microsoft Defender for Endpoint allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-54123
Microsoft-- Microsoft Dynamics 365 (on- premises) version 9.1	Exposure of sensitive information to an unauthorized actor in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-66301
Microsoft-- Microsoft Dynamics 365 Business Central 2024 Release Wave 2	Missing authorization in Dynamics Business Central allows an authorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-40375
Microsoft-- Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-08-11	5.4	CVE-2026-70339
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Deserialization of untrusted data in Microsoft Exchange Server allows an authorized attacker to deny service over a network.	2026-08-11	6.5	CVE-2026-62912
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Missing authorization in Microsoft Exchange Server allows an authorized attacker to bypass a security feature over a network.	2026-08-11	6.5	CVE-2026-62915
Microsoft-- Microsoft Exchange Server	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	2026-08-11	6.5	CVE-2026-65813

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
2016 Cumulative Update 23				
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Server-side request forgery (ssrf) in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	6.5	CVE-2026-58639
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Relative path traversal in Microsoft Office SharePoint allows an authorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-62837
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Insufficiently protected credentials in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	6.5	CVE-2026-62839
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Incorrect authorization in Microsoft Office SharePoint allows an authorized attacker to perform tampering over a network.	2026-08-11	6.5	CVE-2026-63512
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	6.5	CVE-2026-63516
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper control of generation of code ('code injection') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	6.5	CVE-2026-65660
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper input validation in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	4.6	CVE-2026-62917
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	4.6	CVE-2026-64897
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	4.6	CVE-2026-64902
Microsoft-- Microsoft SharePoint	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	4.6	CVE-2026-64916

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Enterprise Server 2016				
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	4.6	CVE-2026-64922
Microsoft-- Microsoft SharePoint Server 2019	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-08-11	4.6	CVE-2026-62829
Microsoft-- Microsoft Teams for iOS	Exposure of sensitive information to an unauthorized actor in Microsoft Teams Mobile allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-65769
Microsoft-- OneDrive for MacOS	Improper link resolution before file access ('link following') in Microsoft OneDrive allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-65680
Microsoft--Visual Studio Code	Improper neutralization of special elements used in a command ('command injection') in Visual Studio Code allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-47285
Microsoft-- Windows 10 Version 1607	Null pointer dereference in Microsoft Remote Registry Service allows an authorized attacker to deny service over a network.	2026-08-11	6.5	CVE-2026-59138
Microsoft-- Windows 10 Version 1607	Null pointer dereference in Microsoft Remote Registry Service allows an authorized attacker to deny service over a network.	2026-08-11	6.5	CVE-2026-61345
Microsoft-- Windows 10 Version 1607	Out-of-bounds read in Remote Desktop Client allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-61918
Microsoft-- Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows DNS allows an authorized attacker to execute code over a network.	2026-08-11	6.6	CVE-2026-61920
Microsoft-- Windows 10 Version 1607	Out-of-bounds read in Remote Desktop Client allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-61921
Microsoft-- Windows 10 Version 1607	Out-of-bounds read in Remote Desktop Client allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-61924
Microsoft-- Windows 10 Version 1607	Heap-based buffer overflow in Windows Universal Disk Format File System Driver (UDFS) allows an unauthorized attacker to execute code with a physical attack.	2026-08-11	6.8	CVE-2026-62699
Microsoft-- Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows DHCP Server allows an unauthorized attacker to disclose information over an adjacent network.	2026-08-11	6.5	CVE-2026-62714
Microsoft-- Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows DHCP Server allows an unauthorized attacker to disclose information over an adjacent network.	2026-08-11	6.5	CVE-2026-62715

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows DHCP Server allows an unauthorized attacker to disclose information over an adjacent network.	2026-08-11	6.5	CVE-2026-62716
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows DHCP Server allows an unauthorized attacker to disclose information over an adjacent network.	2026-08-11	6.5	CVE-2026-62718
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows DHCP Server allows an unauthorized attacker to disclose information over an adjacent network.	2026-08-11	6.5	CVE-2026-62720
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows DHCP Server allows an unauthorized attacker to disclose information over an adjacent network.	2026-08-11	6.5	CVE-2026-62742
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows DHCP Server allows an unauthorized attacker to disclose information over an adjacent network.	2026-08-11	6.5	CVE-2026-62745
Microsoft--Windows 10 Version 1607	Partial string comparison in Windows HTTP Protocol Stack allows an unauthorized attacker to perform tampering over an adjacent network.	2026-08-11	6.5	CVE-2026-62750
Microsoft--Windows 10 Version 1607	Numeric truncation error in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-62769
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows SMB Client allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-62782
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows DHCP Server allows an unauthorized attacker to disclose information over an adjacent network.	2026-08-11	6.5	CVE-2026-62814
Microsoft--Windows 10 Version 1607	Numeric truncation error in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-62881
Microsoft--Windows 10 Version 1607	Numeric truncation error in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-62883
Microsoft--Windows 10 Version 1607	Buffer over-read in Windows SMB Client allows an unauthorized attacker to disclose information over a network.	2026-08-11	6.5	CVE-2026-65794
Microsoft--Windows 10 Version 1607	No cwe for this issue in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-65795
Microsoft--Windows 10 Version 1607	Numeric truncation error in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-65797
Microsoft--Windows 10 Version 1607	Numeric truncation error in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-65798
Microsoft--Windows 10 Version 1607	Integer overflow or wraparound in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-65799

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-70304
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-08-11	6.7	CVE-2026-70330
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows Encrypting File System (EFS) allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-59128
Microsoft--Windows 10 Version 1607	No cwe for this issue in AMD Zen allows an authorized attacker to disclose information locally.	2026-08-11	5.6	CVE-2026-59130
Microsoft--Windows 10 Version 1607	No cwe for this issue in AMD Zen allows an authorized attacker to disclose information locally.	2026-08-11	5.6	CVE-2026-59131
Microsoft--Windows 10 Version 1607	Weak authentication in Microsoft Windows Search Component allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-59135
Microsoft--Windows 10 Version 1607	Use of uninitialized resource in Microsoft COM for Windows allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-59136
Microsoft--Windows 10 Version 1607	Use of uninitialized resource in Windows Event Logging Service allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-59137
Microsoft--Windows 10 Version 1607	Buffer over-read in Windows Event Logging Service allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-61347
Microsoft--Windows 10 Version 1607	Untrusted pointer dereference in Windows GDI allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-61360
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to disclose information locally.	2026-08-11	5	CVE-2026-61368
Microsoft--Windows 10 Version 1607	Cleartext storage of sensitive information in Windows Hello allows an authorized attacker to perform tampering locally.	2026-08-11	5.5	CVE-2026-61928
Microsoft--Windows 10 Version 1607	Use of uninitialized resource in Windows GDI+ allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62709
Microsoft--Windows 10 Version 1607	Buffer over-read in Windows Wired AutoConfig Service allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62730
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows Management Instrumentation allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62738
Microsoft--Windows 10 Version 1607	Use of uninitialized resource in Windows Imaging Component allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62740

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows Win32K allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62743
Microsoft--Windows 10 Version 1607	Buffer over-read in Windows Win32K allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62746
Microsoft--Windows 10 Version 1607	Improper verification of cryptographic signature in Windows Schannel allows an unauthorized attacker to bypass a security feature over a network.	2026-08-11	5.3	CVE-2026-62757
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows Win32K allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62786
Microsoft--Windows 10 Version 1607	Buffer over-read in Windows NTFS allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62793
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62796
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62887
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows GDI allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-65662
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-65784
Microsoft--Windows 10 Version 1607	Buffer over-read in Windows Network File System allows an unauthorized attacker to deny service over a network.	2026-08-11	5.9	CVE-2026-68819
Microsoft--Windows 10 Version 1607	Buffer over-read in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack.	2026-08-11	4.6	CVE-2026-61350
Microsoft--Windows 10 Version 1809	Missing authorization in Windows Defender Firewall Service allows an authorized attacker to bypass a security feature locally.	2026-08-11	5.5	CVE-2026-61936
Microsoft--Windows 10 Version 1809	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62703
Microsoft--Windows 10 Version 21H2	Null pointer dereference in Windows Graphics Kernel allows an unauthorized attacker to deny service over a network.	2026-08-11	6.8	CVE-2026-62702
Microsoft--Windows 11 version 23H2	Untrusted pointer dereference in Windows Win32K allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62798
Microsoft--Windows 11 version 23H2	Inadequate encryption strength in Windows Active Directory allows an authorized attacker to bypass a security feature over a network.	2026-08-11	5.3	CVE-2026-65777

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 11 Version 24H2	Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges with a physical attack.	2026-08-11	6.4	CVE-2026-62708
Microsoft--Windows 11 Version 24H2	Uncontrolled resource consumption in Windows DHCP Client allows an unauthorized attacker to deny service over an adjacent network.	2026-08-11	6.5	CVE-2026-65785
Microsoft--Windows 11 Version 24H2	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-61933
Microsoft--Windows 11 Version 24H2	Improper link resolution before file access ('link following') in Windows Management Services allows an authorized attacker to deny service locally.	2026-08-11	5.5	CVE-2026-70348
Microsoft--Windows 11 version 26H1	Incorrect authorization in Windows Container Isolation FS Filter Driver (unionfs.sys) allows an authorized attacker to disclose information locally.	2026-08-11	5.5	CVE-2026-62775
Microsoft--Windows 11 version 26H1	Improper link resolution before file access ('link following') in Windows Container Isolation FS Filter Driver (unionfs.sys) allows an authorized attacker to perform tampering locally.	2026-08-11	5.5	CVE-2026-72971
migration-planner--migration-planner	A flaw was found in migration-planner. Insufficient validation of the `AgentStatusUpdate.CredentialUrl` field allows an authenticated attacker to store a malicious `javascript:` URL. When a victim views this URL in the Hybrid Cloud Console, it can lead to Cross-Site Scripting (XSS), enabling script execution in the victim's session and potentially disclosing sensitive information.	2026-08-14	6.3	CVE-2026-53472
Ministry of Justice--UYAP Document Editor	Improper restriction of XML external entity reference vulnerability in Ministry of Justice UYAP Document Editor allows Serialized Data External Linking. This issue affects UYAP Document Editor: from 4.5.17 before 5.4.17.	2026-08-12	6.3	CVE-2026-16999
Mintplex-Labs--anything-llm	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. From 1.0.0 to 1.15.0, AnythingLLM's unauthenticated account-recovery flow in server/utls/PasswordRecovery/index.js uses recoverAccount() to deduplicate the raw recoveryCodes values before trimming them, so one valid code submitted twice with different surrounding whitespace can satisfy the two-code check. Each normalized value can also match the same stored hash instead of consuming a distinct hash. An attacker who knows the target username and one recovery code can call POST /api/system/recover-account in multi-user mode, receive a password-reset token, and use POST /api/system/reset-password to take over the account, including an administrator account.	2026-08-10	5.9	CVE-2026-72917
MongoDB--Atlas SQL ODBC Driver	MongoDB Schema Manager and MongoDB Atlas SQL ODBC Driver do not validate the scheme of the authorization and token endpoints returned by an OIDC issuer's discovery document. A user induced to connect to an uncontrolled MongoDB deployment using MONGODB-OIDC authentication may have an uncontrolled URI dispatched to their operating system's default protocol handler, potentially exposing credentials or, under certain conditions, resulting in code execution in the user's context.	2026-08-12	4.8	CVE-2026-19503
MongoDB--BI Connector ODBC Driver	The MongoDB BI Connector ODBC Driver converts floating point column values into text without checking that the result fits within the destination buffer. When an application reads a sufficiently large floating point value as text, the driver may write beyond the end of that buffer and corrupt adjacent memory. A user who can store data in a collection read through the BI Connector could use this to crash the application performing the read.	2026-08-12	6.5	CVE-2026-18888

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MongoDB-- MongoDB Driver	A MongoDB driver component could write sensitive configuration information, including a credential used for outbound network connectivity, to application log output in cleartext during routine client initialization. This occurs automatically as part of normal operation and requires no special privileges to trigger. A party able to read the affected application's logs or downstream log-aggregation storage could recover the credential and reuse it to authenticate to the associated network infrastructure. This issue affects confidentiality only.	2026-08-11	6.5	CVE-2026-18710
MongoDB-- MongoDB Server	An issue in MongoDB Server's handling of certain query predicates against time-series collections with a metaField could allow an authenticated user with write access to cause the server process to terminate unexpectedly, resulting in a denial of service.	2026-08-11	6.5	CVE-2026-18695
MongoDB-- MongoDB Server	An issue in MongoDB Server's applyOps command could allow an authenticated user with specific non-default privileges to perform certain data-definition operations, such as dropping or modifying collections, against collections they do not have permission to manipulate. This is due to an inconsistency in how the target collection is determined between the authorization check and the actual operation.	2026-08-11	6.5	CVE-2026-18696
MongoDB-- MongoDB Server	An issue in MongoDB Server's query planner could allow an authenticated user with read-level privileges to cause the server process to terminate unexpectedly by submitting a specially formed query against a collection with a text index. This could result in a denial of service, affecting connected clients and in-flight operations.	2026-08-11	6.5	CVE-2026-18699
MongoDB-- MongoDB Server	An issue in MongoDB Server's geospatial validation could allow an authenticated user with write privileges to cause an internal reference to be used after the underlying memory has been freed, through concurrent operations against a collection using a certain type of validator. This could result in a server crash, leading to a denial of service.	2026-08-11	6.5	CVE-2026-18700
MongoDB-- MongoDB Server	An issue in MongoDB Server's query subsystem could allow an authenticated user with read privileges to cause the server process to terminate unexpectedly by submitting a specially formed query filter. This could result in a denial of service.	2026-08-11	6.5	CVE-2026-18701
MongoDB-- MongoDB Server	An issue in MongoDB Server could allow an authenticated user with limited, database-scoped privileges to modify diagnostic logging settings that affect the entire server rather than just the intended database. This could allow suppression of diagnostic logging server-wide, potentially obscuring unauthorized activity, or degrade operational monitoring by causing excessive log volume.	2026-08-11	6.4	CVE-2026-18702
MongoDB-- MongoDB Server	An issue in MongoDB Server's aggregation framework could allow an authenticated user with only read privileges to perform write operations against collections they should not be able to modify. This is due to an internal-use aggregation stage being reachable by external clients without an appropriate authorization check on its embedded operations.	2026-08-11	6.5	CVE-2026-18704
MongoDB-- MongoDB Server	An issue in MongoDB Server's Atlas Vector Search feature could allow an authenticated user with read access to one view to retrieve documents from a different, protected view over the same underlying collection. This is due to insufficient handling of certain user-supplied fields when constructing an internal request forwarded to the search process.	2026-08-11	6.5	CVE-2026-18705
MongoDB-- MongoDB Server	An issue in MongoDB Server's \$graphLookup aggregation stage could allow an authenticated user able to issue aggregation and memory-management commands to cause an internal reference to be used after the underlying memory has been freed. This could result in a server crash or, potentially, execution of unintended code.	2026-08-11	6.6	CVE-2026-18706

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MongoDB--MongoDB Server	An issue in MongoDB Server's JavaScript scripting engine could allow an authenticated user with write privileges to cause code they control to be executed within the query scope of other users, through a specially crafted stored value processed during an internal maintenance cycle. This could result in corruption of query results affecting other users and denial of service targeted at their operations on the same database. Impact is limited to the scripting engine's execution sandbox, which does not provide access to database, filesystem, or network resources.	2026-08-11	6.4	CVE-2026-18708
MongoDB--MongoDB Server	An issue in MongoDB Server could allow an authenticated user with direct network access to a shard to improperly commit or abort an in-progress prepared transaction, bypassing the intended transaction coordination process. This could result in cross-shard data inconsistency, cluster clock corruption, and violation of transaction atomicity guarantees.	2026-08-11	6.4	CVE-2026-18709
MongoDB--MongoDB Server	An issue in MongoDB Server could allow an authenticated user with a limited database-scoped role to perform an action against protected system collections that should require more specific privileges. This could result in exposure of collection metadata and, on certain deployment configurations, unauthorized modification of system collection data.	2026-08-11	5.4	CVE-2026-18698
MongoDB--MongoDB Server	An issue in MongoDB Server could allow a party with a valid client certificate and a corresponding user account to authenticate using a certificate-based authentication method, even when an administrator has configured the server to restrict authentication to other mechanisms. This could allow authentication through a method the administrator intended to disable.	2026-08-11	4.2	CVE-2026-18703
MongoDB--MongoDB Server	An issue in MongoDB Server could allow an authenticated user, including one with no assigned privileges, to cause the server process to terminate unexpectedly by submitting a specially formed aggregation command. This could result in a denial of service.	2026-08-11	4.3	CVE-2026-18707
MongoDB--Schema Builder CLI	MongoDB SQL Schema Builder CLI records its startup configuration to standard output and, when file logging is enabled, to a log file on disk. Certain connection settings were written without redaction, so authentication material supplied by the operator could appear in plaintext in that diagnostic output. A local user with read access to the terminal session or the log directory, or anyone with access to a location where those logs are subsequently collected, could obtain those values.	2026-08-12	5.5	CVE-2026-19502
Nagios Enterprises, LLC--Nagios Core	Nagios Core before 4.5.14 and Nagios XI before 2026R1.7 are vulnerable to reflected cross-site scripting in cmd.cgi via the NagFormId parameter. An unauthenticated remote attacker can craft a malicious link that, when followed by an authenticated user, executes arbitrary JavaScript in the victim's browser.	2026-08-12	6.1	CVE-2026-48550
Nagios Enterprises, LLC--Nagios Core	Nagios Core before 4.5.14 and Nagios XI before 2026R1.7 are vulnerable to DOM-based cross-site scripting in jquery.js. Unencoded JSON string values reflected from stored fields are inserted into the DOM without sanitization, allowing attackers to run arbitrary JavaScript in the victim's browser.	2026-08-12	5.4	CVE-2026-48552
NetBox Labs--NetBox	NetBox 4.5.8 contains an ORM injection vulnerability that allows authenticated attackers, including those with read-only API tokens, to inject arbitrary Django ORM lookup expressions into nested object references by supplying crafted JSON dictionary keys in POST, PUT, or PATCH requests to any REST API endpoint. Attackers can exploit the unrestricted queryset used by WritableNestedSerializer to perform boolean-based blind data extraction of sensitive field values and bypass object-level permissions across all application modules including dcim, ipam, tenancy, virtualization, circuits, and extras.	2026-08-11	6.5	CVE-2026-69117
netty--netty	Netty is an asynchronous, event-driven network application framework. Prior to 4.1.136.Final and 4.2.16.Final, io.netty.handler.codec.dns.AbstractDnsRecord, io.netty.handler.codec.dns.DefaultDnsRecordDecoder.decodeRecord(), and io.netty.handler.codec.dns.DnsCodecUtil.decompressDomainName() failed to	2026-08-13	5.3	CVE-2026-73508

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	release retained or newly allocated ByteBuf objects when IDN.toASCII() or encodeDomainName() rejected a malformed domain name, allowing unauthenticated remote DNS packets to leak direct memory incrementally until denial of service. This issue is fixed in versions 4.1.136.Final and 4.2.16.Final.			
Nexcess--GiveWP	Donor Cross Site Scripting (XSS) in GiveWP < 4.16.6 versions.	2026-08-13	6.5	CVE-2026-73357
Nexcess--GiveWP	Unauthenticated Broken Access Control in GiveWP < 4.16.6 versions.	2026-08-13	5.3	CVE-2026-73349
nextauthjs--next-auth	NextAuth.js provides authentication for Next.js. Prior to @auth/core 0.41.3 and next-auth 4.24.15 and 5.0.0-beta.32, Auth.js stores the OAuth/OIDC anti-CSRF checks state, nonce, and the PKCE verifier in global cookies that are not bound to the provider that created them. On callback, a check value minted during a sign-in started with one provider can satisfy the callback for a different provider because the stored cookie is not verified against the callback provider's identity, including the provider ID, issuer, client ID, or redirect URI. In a multi-provider application that permits account linking while logged in, when one provider's authorization request is observable and a target provider callback can be satisfied without a PKCE verifier, an attacker can lure a victim into starting a legitimate same-origin flow and link the attacker's target-provider account to the victim's Auth.js user. The linked provider grants the attacker persistent sign-in to the victim's account, while cross-site request forgery alone is insufficient. This issue is fixed in @auth/core 0.41.3 and next-auth 4.24.15 and 5.0.0-beta.32.	2026-08-12	6.8	CVE-2026-73419
Nmap Project--Nmap	Nmap versions up to and including 7.99 contains a denial of service vulnerability that allows remote attackers to crash the application by sending a crafted packet containing a zero-length TCP option. The malformed packet forces the Packet:parse_options() function in nselib/packet.lua to allocate objects in an infinite loop, causing an out-of-memory condition that results in application crash.	2026-08-11	6.5	CVE-2026-72712
NodeBB--NodeBB	NodeBB before 4.15.0 contains a stored cross-site scripting vulnerability in the renderEmoji function that fails to escape tag.icon.url and tag.name attributes. Attackers can deliver malicious ActivityPub Create/Note objects with crafted emoji tags to inject arbitrary HTML and JavaScript into stored post content, executing code in all viewers' browsers.	2026-08-13	6.1	CVE-2026-73038
NortheBridge--luminalshine	NortheBridge/luminalshine is a Sunshine-compatible game stream host for Moonlight. Prior to version 26.05.0-rc4, a latent gap exists on a default install, the file at `src/platform/windows/misc.cpp` lives at `C:\ProgramData\LuminalShine\config\apps.json` and is created by the `SYSTEM` service. Under Windows' default `C:\ProgramData` inheritance, that gives `BUILTIN\Users` only Read+Execute - not writable - so the canonical EoP doesn't actually trigger on a vanilla install. Version 26.05.0-rc4 contains a patch for the issue. As a workaround, use default csidlib DACls for `ProgramData`.	2026-08-12	6.3	CVE-2026-50544
Nozomi Networks--Arc	A path traversal vulnerability was discovered in the Offline archives functionality of the local web interface due to insufficient validation of an input parameter. A local user with administrative credentials for the web interface could submit an archive name containing traversal sequences and delete arbitrary files reachable by the Arc process, which runs with administrative privileges on the host.	2026-08-11	6	CVE-2026-33922
Nozomi Networks--Arc	The Windows installer deployed Npcap leaving its access restriction option at the insecure default value, so the driver was accessible to every local user of the host instead of being restricted to administrators only. A local user without administrative privileges could use the Npcap driver to capture the traffic reaching the host, which discloses information belonging both to the host and to other systems on the same network segment, and to send arbitrary raw packets on that segment.	2026-08-11	5.2	CVE-2026-33921
nuxt--nuxt	Nuxt versions >= 4.4.7 and < 4.5.1, and >= 3.21.7 and < 3.21.10, contain an information disclosure vulnerability in the development server's Chrome DevTools workspace endpoint (GET /.well-known/appspecific/com.chrome.devtools.json).	2026-08-11	6.2	CVE-2026-72744

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The endpoint's local-request gate (isLocalDevRequest) is header-based and trusts the attacker-supplied Host header rather than the connected peer address. When the dev server is bound to a network-reachable interface (e.g. nuxt dev --host) and experimental.chromeDevtoolsProjectSettings is enabled (the default), an unauthenticated attacker on the LAN can send a request with a spoofed Host header and no browser-specific headers (Sec-Fetch-Site, Origin, Referer) to retrieve the project's absolute filesystem root path (rootDir) and a persistent per-project workspace UUID. Production builds are unaffected. Fixed in 4.5.1 and 3.21.10.			
ondata--ckan-mcp-server	CKAN MCP Server is a tool for querying CKAN open data portals. Prior to 0.4.112, canonicalizeParams in src/utls/cache.ts serializes request parameters with unescaped ampersand, equals-sign, and vertical-bar delimiters, allowing different logical parameter sets used by buildCacheKey to collide and an attacker to prime a shared cache with a response for a victim's distinct query. This issue is fixed in version 0.4.112.	2026-08-14	6.5	CVE-2026-73846
ondata--ckan-mcp-server	CKAN MCP Server is a tool for querying CKAN open data portals. Prior to 0.4.112, the ckan_get_mqa_quality and ckan_get_mqa_quality_details tools in src/tools/quality.ts use isValidMqaServer to validate the server_url parameter with a prefix-only regular expression for dati.gov.it, allowing suffix-host and URL-userinfo values to target an attacker-controlled host and return a spoofed response. This issue is fixed in version 0.4.112.	2026-08-14	5.3	CVE-2026-73845
OP-TEE--optee_os	OP-TEE OS through 4.10.0, fixed in commit 8794043, contains a use-after-free vulnerability in the Trusted Application loader that allows attackers with the ability to load a signed Trusted Application to corrupt secure-world kernel memory by setting the TA_FLAG_CONCURRENT flag in a user TA signed header. Attackers can cause two concurrent sessions to operate on the same shared context without locking, corrupting the uctx->vm_info.regions list during memref parameter mapping and unmapping to free vm_region nodes still in use, resulting in a use-after-free in S-EL1 secure-world kernel memory.	2026-08-10	6.7	CVE-2026-71968
OP-TEE--optee_os	OP-TEE OS through 4.10.0, fixed in commit 7b8b494, contains a buffer underwrite vulnerability in the RSA NOPAD encrypt and decrypt operations within the mbedTLS software backend and SE050 hardware driver that allows a malicious Trusted Application to corrupt secure-world heap memory by supplying an input length exceeding the RSA modulus size. When src_len exceeds rsa_len, the subtraction expression wraps to a large unsigned value, causing a subsequent memcpy to write attacker-controlled data before the destination buffer in S-EL1 secure-world heap memory.	2026-08-10	6.7	CVE-2026-71969
OP-TEE--optee_os	OP-TEE OS through 4.10.0, fixed in commit 0aadfc2, contains a null pointer dereference vulnerability in the Widevine pseudo-TA open_session handler that allows Normal World clients to cause a denial of service when CFG_WIDEVINE_PTA is enabled. Attackers can open a session directly on the Widevine PTA to trigger an unconditional dereference of a NULL calling session pointer via is_user_ta_ctx(), faulting the TEE at S-EL1 and crashing the trusted execution environment.	2026-08-10	5.5	CVE-2026-71967
Open5GS--Open5GS	A vulnerability was found in Open5GS up to 2.7.1. This affects the function hss_ogs_diam_s6a_air_cb/hss_ogs_diam_s6a_ulr_cb of the file src/hss/hss-s6a-path.c of the component Diameter S6a Interface. Performing a manipulation of the argument os.len results in stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been made public and could be used. Upgrading to version 2.7.2 is able to mitigate this issue. The patch is named e89aa79efe629ae90f59dcdf8847c117d9a7da86. It is suggested to upgrade the affected component.	2026-08-11	6.3	CVE-2024-14042
Open5GS--Open5GS	A vulnerability was determined in Open5GS up to 2.7.1. This vulnerability affects the function mme_s6a_subscription_data_from_avp of the file src/mme/mme-fd-path.c of the component Diameter S6a Interface. Executing a manipulation of the argument msisdn_len can lead to heap-based buffer overflow. It is possible to	2026-08-11	6.3	CVE-2024-14043

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	launch the attack remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.7.2 is able to resolve this issue. This patch is called 7ea82cb87bb65c3694d8d7c7a5efed1c4d3c9304. Upgrading the affected component is recommended.			
Open5GS-- Open5GS	A vulnerability was identified in Open5GS up to 2.7.1. This issue affects the function pcrf_rx_aar_cb of the file src/pcrf/pcrf-rx-path.c of the component Diameter Rx Handler. The manipulation of the argument num_of_media_component/num_of_sub leads to buffer overflow. The attack can be initiated remotely. The exploit is publicly available and might be used. Upgrading to version 2.7.2 is capable of addressing this issue. The identifier of the patch is 87b4e4535c77ded627cdb6f4e4e2e3ea761f40b7. It is recommended to upgrade the affected component.	2026-08-12	6.3	CVE-2024-14044
Open5GS-- Open5GS	A flaw has been found in Open5GS up to 2.7.1. Affected by this vulnerability is an unknown functionality of the component freeDiameter. This manipulation causes memory corruption. The attack is possible to be carried out remotely.	2026-08-12	6.3	CVE-2025-15685
Open5GS-- Open5GS	A vulnerability was detected in Open5GS up to 2.7.6. Affected is the function diam_log_func of the file lib/diameter/common/init.c of the component CER Handler. The manipulation results in reachable assertion. The attack can be executed remotely. The exploit is now public and may be used. Upgrading to version 2.7.7 is able to address this issue. The patch is identified as c1a803516a3c0485696cb9bcca7a80ad857c7383. It is advisable to upgrade the affected component.	2026-08-12	5.3	CVE-2025-15684
Open5GS-- Open5GS	A vulnerability has been found in Open5GS up to 2.7.6. Affected by this issue is the function fd_msg_sess_get of the component HSS Service. Such manipulation of the argument Session-Id leads to denial of service. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project locked and limited conversation to collaborators.	2026-08-12	4.3	CVE-2025-15686
Open5GS-- Open5GS	A security flaw has been discovered in Open5GS up to 2.7.6. Impacted is the function smf_gx_cca_cb of the component SMF Diameter Gx Credit-Control-Answer Handler. The manipulation results in denial of service. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 2.7.7 is recommended to address this issue. The patch is identified as f23d7a5e959acd8f37b925dc29b85f26b7d391cb. Upgrading the affected component is advised.	2026-08-12	4.3	CVE-2025-15687
OpenBoxes-- OpenBoxes	A vulnerability was found in OpenBoxes up to 0.9.7. The impacted element is the function Upload of the file rails-app/controllers/org/pih/warehouse/product/ProductController.groovy of the component Product Upload Endpoint. Performing a manipulation of the argument params.url results in server-side request forgery. The attack is possible to be carried out remotely. The exploit has been made public and could be used. Upgrading to version 0.9.8-hotfix1 and 0.9.8 is sufficient to resolve this issue. The patch is named a599007325efe780a21b3537ecce3ca25635c926. It is suggested to upgrade the affected component.	2026-08-16	6.3	CVE-2026-19927
OpenBoxes-- OpenBoxes	A vulnerability was determined in OpenBoxes up to 0.9.7. This affects the function needManager of the file rails-app/controllers/org/pih/warehouse/RoleInterceptor.groovy of the component Role Interceptor. Executing a manipulation can lead to improper privilege management. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.9.8-hotfix1 and 0.9.8 mitigates this issue. This patch is called 788cace0af816aa972a713a4631c57f16f895e6b. Upgrading the affected component is recommended.	2026-08-16	6.3	CVE-2026-19928

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
OpenBoxes-- OpenBoxes	A vulnerability was identified in OpenBoxes up to 0.9.6. This impacts the function buildZebraTemplate of the file grails-app/controllers/org/pih/warehouse/core/DocumentController.groovy of the component Template Processing. The manipulation leads to improper neutralization of special elements used in a template engine. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. Upgrading to version 0.9.8-hotfix1 and 0.9.8 will fix this issue. The identifier of the patch is deec6a4a7aba86ce99c4bda37142e41d209293e. It is recommended to upgrade the affected component.	2026-08-16	6.3	CVE-2026-19929
OpenBSD-- OpenSSH	In ssh in OpenSSH before 10.5, a use-after-free for realloc data can occur if a certain pair of remote-forwarding operations are concurrent.	2026-08-11	4.8	CVE-2026-73282
openchoreo-- openchoreo	OpenChoreo is a complete, open-source developer platform for Kubernetes. Prior to 1.0.3, 1.1.3, and 1.2.0-rc.2, the POST /api/v1alpha1/autobuild endpoint in internal/openchoreo-api/api/handlers/webhook_handler.go selected a webhook provider from caller-controlled X-Event-Key, accepted Bitbucket requests without HMAC-SHA256 in X-Hub-Signature or a configured bitbucket-secret, and allowed unauthenticated build triggers for components matched by repository URL and branch, including cross-provider triggers using attacker-supplied commit SHAs. This issue is fixed in versions 1.0.3, 1.1.3, and 1.2.0-rc.2.	2026-08-13	5.3	CVE-2026-73840
OpenIMSDK-- OpenIM Server (open-im-server)	OpenIM Server v3.8.3 contains a missing authorization vulnerability that allows any authenticated user to access admin-only management API endpoints by submitting POST requests with a regular user bearer token to /user/get_users, /user/get_all_users_uid, and /group/get_groups. Attackers can exploit the absent authverify.CheckAdmin() call in the GetPaginationUsers, GetAllUserID, and GetGroups handlers to enumerate all platform user accounts including userIDs, nicknames, and manager level flags, as well as all groups including private groups the user has never joined, exposing group names, owner IDs, and member counts.	2026-08-11	6.5	CVE-2026-69115
openremote-- openremote	OpenRemote notification deletion endpoints fail to enforce realm boundaries, allowing any realm administrator to delete notifications belonging to other realms. Attackers with write:admin role in one realm can send DELETE requests to remove notifications from the master realm or other tenants without authorization checks.	2026-08-13	6.5	CVE-2026-73616
OpenSignLabs-- OpenSign	An information disclosure vulnerability in OpenSignLabs OpenSign through 2.37.0 allows unauthenticated remote attackers to map any email address or username to its internal user objectId via the getUserId Parse cloud function. The function performs no authentication before resolving and returning the internal identifier. An attacker can use this to enumerate user accounts and target subsequent attacks.	2026-08-11	5.3	CVE-2026-72549
OpenStack-- Designate	In OpenStack Designate before 22.0.2, the mDNS handler performs pool-blind lookups when resolving record queries and NOTIFY requests. When two zones with the same name exist across different pools, the lookup fails with a deterministic error, causing the handler to return REFUSED for all DNS queries through that path. The _handle_notify path is exploitable via a single unauthenticated UDP packet. This is independently reachable through the cross-tenant zone overlap described in a different recent CVE, and also affects legitimate same-tenant cross-pool configurations. BIND9 views do not mitigate this issue as mDNS is a shared service upstream of any view configuration.	2026-08-12	6.8	CVE-2026-71194
OpenStack-- Ironic	In OpenStack Ironic before 38.0.1, the autodetect deploy interface may fail to run cleaning immediately after enrollment with, or changing to, the autodetect deploy interface.	2026-08-14	6.3	CVE-2026-74250
OpenStack-- Octavia	OpenStack Octavia through 18.0.0 mishandles quality of service (QoS) policy authorization. By associating another project's QoS policy with an amphora, an authenticated user may prevent deletion of that policy. All Octavia deployments are affected.	2026-08-14	4.3	CVE-2026-74248

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opentofu-- opentofu	OpenTofu before 1.11.7 fails to validate existing symlinks in the provider cache directory during initialization. Attackers can place a malicious symlink in a trusted working directory to cause tofu init to write provider package contents to arbitrary filesystem locations outside the working tree.	2026-08-16	6.1	CVE-2026-74796
oscal-compass-- compliance-trestle	compliance-trestle is a tooling platform for managing compliance as code. Prior to versions 3.12.2 and 4.0.3, the HTTPSFetcher._do_fetch() method passes a user-supplied URL directly to requests.get() without validation. This allows an attacker to perform Server-Side Request Forgery, targeting internal services or cloud metadata endpoints. Versions 3.12.2 and 4.0.3 fix the issue.	2026-08-14	6.7	CVE-2026-46380
owen2345-- CamaleonCMS	CamaleonCMS 2.9.1 contains a server-side template injection vulnerability that allows authenticated administrators to execute arbitrary commands by embedding ERB tags in the email parameter of the test_email settings action, which are evaluated when an SMTP rejection reflects the recipient address back in the exception message rendered as an inline ERB template. Attackers can submit a crafted email parameter containing ERB expressions through the admin settings test_email endpoint, causing the Rails inline template renderer to evaluate attacker-controlled Ruby code and achieve arbitrary command execution as the Rails process user.	2026-08-12	6.6	CVE-2026-73330
owen2345-- CamaleonCMS	CamaleonCMS version 2.9.2 and earlier contains a missing authorization vulnerability in the admin users controller that allows any authenticated user to access any other user's profile data by supplying an arbitrary user ID parameter. Attackers can send a GET request to the admin profile endpoint with an enumerable sequential integer user ID to disclose profile information of any user, including administrators, due to the profile action being excluded from the role validation filter with no compensating ownership check.	2026-08-11	4.3	CVE-2026-56720
Passionate Programmer Peter-- WP Data Access	Author Cross Site Scripting (XSS) in WP Data Access <= 5.5.79 versions.	2026-08-13	5.9	CVE-2026-73344
Payment Button for PayPal-- Payment Button for PayPal	The Payment Button for PayPal WordPress plugin through 1.2.3.44 does not enforce the merchant-configured price server-side and trusts a client-supplied payment amount, allowing unauthenticated attackers to create a real PayPal order against the merchant for an arbitrary lower amount.	2026-08-12	5.3	CVE-2026-16990
Payment Gateway-- Payment Gateway for PayPal on WooCommerce	The Payment Gateway for PayPal on WooCommerce WordPress plugin before 9.2.1 does not verify that payment actually succeeded before completing an order in its PayPal return handler: it reads attacker-controlled parameters, performs no amount comparison and no order-ownership check, and completes the order even when the server-side gateway verification fails, allowing an unauthenticated attacker to mark arbitrary orders as paid without paying.	2026-08-12	5.3	CVE-2026-16621
pdamsten-- Fullscreen Galleria	The Fullscreen Galleria plugin for WordPress is vulnerable to generic SQL Injection via 'href' Attribute in Post Content in all versions up to, and including, 1.6.12 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-16	6.5	CVE-2026-16079
Phoenix Contact-- AXC F 1152	An authenticated attacker with low privileges can access an endpoint in the controller's web interface that is vulnerable to SQL injection. The vulnerability affects a SQLite database used only for storing notification messages. Therefore, the impact is limited to the system's notification functionality.	2026-08-12	4.3	CVE-2025-41771
PhotoPrism-- PhotoPrism	An insecure direct object reference vulnerability in PhotoPrism through commit bb0b933 allows any user with a valid preview token to retrieve the original-resolution cover photo of any album. The AlbumCover handler does not verify that the requesting user is authorized to access the specified album before serving the	2026-08-11	4.3	CVE-2026-72540

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cover image. An attacker with any valid preview token can enumerate and download album cover images belonging to other users.			
phplist--phplist3	phplist before 3.7.0-RC5 fail to enforce CSRF token validation on the bounce rule deletion endpoint (bouncerule.php / bouncerule.php). The deletion is performed via a GET request (?page=bouncerule&del=N), and the central CSRF check (verifyCsrfGetToken) is invoked with enforce=false, so it only validates the token when a 'tk' parameter is present. A remote attacker can trick an authenticated administrator into loading a crafted URL (e.g., embedded in an image tag) to delete arbitrary bounce rules from the phplist_bounceregex table without a valid CSRF token.	2026-08-13	5.4	CVE-2026-73481
picocms--Pico	A host header injection vulnerability in picocms/Pico through 2.1.4 allows an unauthenticated remote attacker to control the origin of JavaScript and CSS assets loaded by the default theme. When base_url is unset (the default), Pico::getBaseUrl in lib/Pico.php builds the base URL from unvalidated Host, X-Forwarded-Host, X-Forwarded-Proto, and X-Forwarded-Port request headers.	2026-08-10	6.1	CVE-2026-72574
PostgreSQL--PostgreSQL	Cleartext storage in PostgreSQL pgcrypto disabled ciphers allows a user to recover cleartext, via direct observation of the faulty ciphertext. The OpenSSL version and OpenSSL configuration determine the disabled ciphers. If the application accepts encrypted data as input, decryption will succeed even with the wrong key. This in turn loses the modest protection from the Modification Detection Code (MDC). Affected functions are pgp_sym_encrypt, pgp_sym_decrypt, pgp_pub_encrypt, pgp_pub_decrypt, pgp_sym_encrypt_bytea, pgp_sym_decrypt_bytea, pgp_pub_encrypt_bytea, and pgp_pub_decrypt_bytea. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	6.5	CVE-2026-14663
PostgreSQL--PostgreSQL	Observable response discrepancy in PostgreSQL SCRAM authentication allows an unauthenticated user to test the existence of a user via observing the SCRAM iteration count. This requires the probed user to have a non-default scram_iterations count, because the authentication challenge for a nonexistent user reports the default scram_iterations. Within major versions 16-18, minor versions before PostgreSQL 18.5, 17.11, and 16.15 are affected. Versions before PostgreSQL 16 are unaffected.	2026-08-13	5.3	CVE-2026-14672
PostgreSQL--PostgreSQL	Incomplete tracking in PostgreSQL of changes to role membership, role attributes, and database ownership allows a query to continue using cached row-level security policies after those changes require a different policy, via plan reuse. Stale policies continue until some other event invalidates the cache or connection termination ends the session. This permits a user to complete reads and modifications that were recently permitted but now forbidden. An attacker must tailor an attack to a particular application's pattern of privilege removal and role-specific row security policies. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	4.2	CVE-2026-14666
PostgreSQL--PostgreSQL	Buffer over-read in PostgreSQL pg_trgm index picksplit function reads past end of a heap buffer. This might allow a table maintainer to infer limited memory values, via the lossy signal of index split choices. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	4.3	CVE-2026-14678
PostgreSQL--PostgreSQL	Improper enforcement of message integrity in PostgreSQL GSSAPI support allows a user to negotiate GSSAPI contrary to pg_hba.conf rules, via initial direct TLS connection. Despite a pg_hba.conf that appears to require GSSAPI, the connection may exchange data over TLS encryption alone. If the TLS settings are more permissive than the GSS settings, the connection may continue with lesser protection. Within major versions 17-18, minor versions before PostgreSQL 18.5 and 17.11 are affected. Versions before PostgreSQL 17 are unaffected.	2026-08-13	4.2	CVE-2026-14681
PostgreSQL--PostgreSQL	Buffer over-read in PostgreSQL ascii() SQL function allows a user to disclose up to 3 bytes after the end of a specific allocation, via a crafted text value. This is the same	2026-08-13	4.3	CVE-2026-18024

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	class of defect that CVE-2026-2006 fixed, though this instance has less impact. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.			
PostgreSQL-- PostgreSQL	Missing authorization in PostgreSQL DDL commands allows an object creator to achieve denial of service against ALTER and DROP of the type, via creating a dependency on the type. Many DDL operations did check the privilege, but assigning a range subtype and referencing the type from an SQL expression did not. Versions before PostgreSQL 18.5, 17.11, 16.15, 15.19, and 14.24 are affected.	2026-08-13	4.3	CVE-2026-6470
Priority--Portal Generator add-on to Priority ERP (developed by Soft Solutions)	CWE-203: Observable Discrepancy	2026-08-13	5.3	CVE-2026-59502
Progress Software Corporation-- WhatsUp Gold	In WhatsUp Gold versions released before 2026.0.2, a privileged attacker can create a LogToFile action specifying an arbitrary file extension within the IIS web root.	2026-08-12	6.8	CVE-2026-65939
Progress Software Corporation-- WhatsUp Gold	In WhatsUp Gold versions released before 2026.0.2, a privileged attacker can write arbitrary files to a web-accessible location on the host server.	2026-08-12	6.8	CVE-2026-65940
Progress Software Corporation-- WhatsUp Gold	In WhatsUp Gold versions released before 2026.0.2, an improper authorization vulnerability in the Scheduled Reports API allows any authenticated user to invoke restricted actions.	2026-08-12	4.3	CVE-2026-65938
properfraction-- Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content ProfilePress	The The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content - ProfilePress plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 4.16.19. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with subscriber-level access and above, to execute arbitrary shortcodes. The partial mitigation introduced via strip_shortcodes() on [profile-first-name] and [profile-last-name] can be bypassed through the [profile-display-name format="first_last_names"] render path, the [profile-bio] render path (which re-fetches the raw description meta), and the double-bracket escape sequence [[tag]], all of which allow attacker-controlled shortcode text to reach the outer do_shortcode() call.	2026-08-16	5.4	CVE-2026-18385
prowler-cloud-- prowler	Prowler is a cloud security platform. Prior to 5.37.0, Prowler's HTML output formatter in prowler/lib/outputs/html/html.py inserted finding.resource_tags, assembled by unroll_dict and parse_html_string, into generated reports without HTML escaping, allowing a cloud principal who can modify a scanned resource tag to store HTML or JavaScript that executes when another user opens the report. This issue is fixed in version 5.37.0.	2026-08-12	5.4	CVE-2026-73262
Quanovate Tech Inc. (operating as Mira / Mira Care)-- Mira Firmware	The Mira hormone monitor device firmware accepts a 0x01 write from any BLE central without authentication, causing the device to reboot into bootloader mode. An attacker could cause a denial-of-service condition or disrupt ovulation tracking and fertility monitoring workflow.	2026-08-11	6.5	CVE-2026-66098
Quanovate Tech Inc. (operating as Mira / Mira Care)-- Mira Firmware	When the Mira Android app opens in-app WebView content (e.g., shop redirect flows), the user's live session token is appended to the URL as a query string parameter, and a persistent user identifier is included in the WebView's User-Agent header. Both are then transmitted to third-party web properties, referrer logs, and any JavaScript running in the WebView context.	2026-08-11	6.5	CVE-2026-66832
Quanovate Tech Inc. (operating as	The Mira cloud authentication endpoints do not enforce per-account rate limiting, per-IP throttling, or account lockout after repeated failed login attempts. An attacker can use brute-force methods to obtain gain access to user accounts.	2026-08-11	5.3	CVE-2026-66340

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mira / Mira Care-- Mira Firmware				
Quanovate Tech Inc. (operating as Mira / Mira Care)-- Mira Firmware	The Mira cloud API accepts the firmware version reported by the companion app as authoritative for a given device, without independently attesting the version from the device itself. An authenticated attacker could submit arbitrary firmware version strings for their own device, allowing them to evade vendor-side vulnerable-fleet analytics, suppress security update prompts to the user, and misrepresent patch-adoption metrics.	2026-08-11	4.3	CVE-2026-64934
quantumcloud-- Slider Hero with Video Background, Animation	The Slider Hero plugin for WordPress is vulnerable to second-order SQL Injection in versions up to, and including, 9.1.7 via the <code>qclد_sliderhero_duplicate()</code> function. Slide data (description, title, btn, btn2, image_link, custom, etc.) is stored safely via <code>\$wpdb->update()</code> with <code>%s</code> placeholders in the <code>qchero_save_image</code> AJAX handler, but when an administrator triggers the 'heroduplicatesslider' task, <code>qclد_sliderhero_duplicate()</code> re-reads every slide column and concatenates the raw values directly into an <code>INSERT VALUES</code> tuple that is then executed with <code>\$wpdb->query()</code> - with no <code>\$wpdb->prepare()</code> , <code>esc_sql()</code> , or <code>_real_escape_string</code> in between. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-16	4.9	CVE-2026-17582
quasarframework-- quasar	Quasar Framework is a framework for building high-performance Vue.js user interfaces. Prior to 2.22.0, the public <code>extend()</code> utility in <code>ui/src/utills/extend/extend.js</code> recursively copied attacker-controlled object keys during <code>extend(true, target, source)</code> deep merges without rejecting an own <code>__proto__</code> property. The merge could descend into the prototype object and write attacker-controlled properties to <code>Object.prototype</code> in the same JavaScript process. Applications that passed user-controlled or partially user-controlled objects to <code>extend()</code> could experience logic bypass, unsafe default-option injection, denial of service, or other application-specific impact when polluted properties were later consumed. This issue is fixed in version 2.22.0.	2026-08-13	5.6	CVE-2026-73647
Quick Paypal Payments--Quick Paypal Payments	The Quick Paypal Payments WordPress plugin through 5.7.50 does not verify the paid amount, receiver, or payment status in its PayPal IPN handler and marks an order paid on an order-token match alone, so a buyer who pays an arbitrary small amount can have a full-price order marked paid.	2026-08-12	5.3	CVE-2026-17008
rainearshine-- npm-check-updates	<code>npm-check-updates</code> through 23.0.2, fixed in commit b554b84, contains a terminal escape sequence injection vulnerability that allows an attacker to embed arbitrary terminal control characters in a dependency's package.json homepage or repository URL fields. When a developer runs <code>ncu</code> with the <code>--format homepage</code> or <code>--format repo</code> option, unfiltered escape sequences are written directly to the terminal, enabling malicious output manipulation or other terminal-dependent effects.	2026-08-10	4.3	CVE-2026-73035
Rapid7-- Velociraptor	Velociraptor's NTFS parsing library mishandles several out of bound and memory exhaustion bugs which may be triggered by maliciously crafted NTFS images. Typically Velociraptor's NTFS parser is used on live NTFS filesystems, limiting the opportunity of attackers corrupting the filesystem. However, in some applications (e.g. dead disk forensics https://docs.velociraptor.app/docs/forensic/deaddisk/) Velociraptor may be used on untrusted NTFS image files. If an attacker is able to inject maliciously corrupted NTFS Volumes they can cause a crash and a Denial of Service.	2026-08-11	6.2	CVE-2026-17535
Rapid7-- Velociraptor	The Velociraptor gRPC API has a <code>VFSGetBuffer</code> endpoint which allows reading files from the datastore. To prevent users from reading sensitive files or accessing other orgs, the requested path is prefix checked against a list of denied prefixes. This prefix check can be bypassed allowing a user to access usually denied files. If the user has read permission in the ROOT org, this allows access to other orgs, in which the user may not have permission.	2026-08-11	6.8	CVE-2026-18636

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Rapid7--Velociraptor	Any authenticated Velociraptor user - including one holding only the readerrole - can terminate the entire server process with a single request, by calling SetPassword with a username that does not exist.	2026-08-11	6.5	CVE-2026-18638
Rapid7--Velociraptor	The hunt_delete() VQL function allows deleting hunts. Velociraptor misapplied the permission check requiring only COLLECT_CLIENT (usually assigned to the "investigator" role) instead of the "DELETE_RESULTS" permission (usually only assigned to "administrators").	2026-08-12	6.5	CVE-2026-64952
Rapid7--Velociraptor	When Microsoft Excel imports a CSV file, it executes cells beginning with certain characters as formulas, giving such CSV files arbitrary execution. Velociraptor fails to sanitize such cells when exporting to CSV from various places such as the GUI, offline collector or data exports. It is not clear if the vulnerability is actually in Microsoft Excel treating a CSV data file as executable content, or if Velociraptor should be sanitizing the data to prevent Excel from executing it. However, since this is such a common use case for Velociraptor we decided to highlight it in an advisory.	2026-08-12	6.1	CVE-2026-64955
Rapid7--Velociraptor	Missing authorization check in the upload_azure, upload_sftp, and upload_smb VQL plugins allows an authenticated analyst-role user can initiate attacker-controlled outbound network connections from the Velociraptor server, bypassing the NETWORK ACL permission boundary. This enables internal network reconnaissance via port oracle and potential data exfiltration to external endpoints.	2026-08-11	4.1	CVE-2026-18348
Rapid7--Velociraptor	Velociraptor allows reading Stacked result sets from the GUI. Velociraptor's multi-tenant design stores sub orgs within the datastore directory. The path requested by the GUI is not correctly checked against the prefix deny list, allowing result sets to read from denied prefixes. In particular, a user with read access to the root org can access result sets from child orgs.	2026-08-12	4.9	CVE-2026-18652
Razinsoft--Ready eCommerce	ReadyCommerce before 4.5.2 contains a stored cross-site scripting (XSS) vulnerability that allows authenticated customers to inject malicious HTML payloads through the chat and support ticket messaging systems by exploiting unsanitized rendering via the v-html directive in Messages.vue, RightChatSidebar.vue, SupportTicketMessages.vue, and SupportTicketDetails.vue. Attackers can submit crafted message content that executes arbitrary JavaScript in the browser of any shop owner or administrator who views the message, enabling session cookie theft and account takeover.	2026-08-10	5.4	CVE-2026-63105
rConfig--rConfig	rConfig before 8.2.13 contains a path traversal vulnerability that allows authenticated attackers to read arbitrary files by supplying unsanitized directory traversal sequences in the filename GET parameter of the download_export() method. Attackers can craft requests with ../ sequences to escape the exports base directory and access sensitive files readable by the web server process, including application environment files containing encryption keys, database credentials, and mail configuration.	2026-08-12	6.5	CVE-2026-64826
Red Hat--Multicluster Engine for Kubernetes	A flaw was found in the provider-credential-controller component of multicluster-engine (MCE). An attacker with specific permissions on the hub cluster, and knowledge of a prior credential value, could exploit an authorization bypass vulnerability. By manipulating `copiedFrom` labels, the attacker could intercept newly rotated provider credentials, leading to unauthorized information disclosure. This allows access to sensitive credentials that should otherwise be protected.	2026-08-12	5.8	CVE-2026-19130
Red Hat--Multicluster Global Hub	A flaw was found in multicluster-global-hub. During a ManagedClusterMigration, the system incorrectly grants all managed hubs read access to a shared communication topic. This allows a compromised managed hub to intercept and collect sensitive bootstrap kubeconfigs, which contain API server tokens intended for other hubs. These tokens have an extended validity of approximately 9.86	2026-08-10	6.3	CVE-2026-71577

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	years, significantly increasing the risk of unauthorized access and information disclosure to other managed clusters.			
Red Hat--Pen Drive Powered by Red Hat Lightspeed	A flaw was found in insights-core where the password redaction layer fails to recognize credentials not keyed under the literal string 'password'. This allows SSSD LDAP bind passwords (ldap_default_authtok) and Pacemaker fence device credentials to be included in cleartext in archives uploaded to console.redhat.com.	2026-08-11	6.5	CVE-2026-19391
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the multicloud-operators-channel component. This vulnerability allows a user with specific permissions to manipulate how the system handles sensitive information, known as Secrets, across different parts of the system (namespaces). By exploiting this, an attacker can modify these Secrets in unauthorized areas. This could lead to unauthorized access to information or elevated privileges within the system.	2026-08-12	6.4	CVE-2026-64927
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in insights-client. When the application receives a non-200 response, it logs the request headers, which can include the cloud.openshift.com pull-secret token. A local user with access to pod logs on the hub could read this long-lived credential. This information disclosure could grant unauthorized access to Red Hat cloud services.	2026-08-11	6.3	CVE-2026-71474
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in insights-client. The setDefault() function logs the value of every environment variable it processes, including CCX_TOKEN, a bearer credential used in disconnected cluster deployments. When glog verbosity is set to level 2 or higher, the token is written in clear text to the pod log on every startup. An attacker with access to pod logs or centralized logging could obtain the credential, leading to unauthorized access to the CCX API.	2026-08-11	6.3	CVE-2026-71845
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in insights-client. The component's ServiceAccount is bound to a ClusterRole granting cluster-wide secrets get, list, and watch permissions, while the code only requires access to a single specific Secret. This excessive privilege means that a compromise of the insights-client pod or ServiceAccount token would grant an attacker read access to all Secrets across the hub cluster, including managed-cluster kubeconfigs and other sensitive credentials.	2026-08-12	6.5	CVE-2026-71846
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in acm-search-v2-api-rhel9. When the 'getFederationConfig' function refreshes its cache, it improperly reuses a user's bearer token for all subsequent federated requests until the cache expires. This allows other authenticated users to gain unauthorized access to remote managed hub search results, leading to information disclosure.	2026-08-11	5.3	CVE-2026-71468
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in insights-client. A compromised managed cluster, referred to as a 'spoke', can inject unencoded data into the Insights API URL path. This occurs because the ClusterID, which is controlled by the spoke, is used directly in the request path without proper validation or URL encoding. This vulnerability allows a malicious spoke to redirect authenticated requests to unintended API endpoints, potentially leading to information disclosure or unauthorized access.	2026-08-11	5	CVE-2026-71475
Red Hat--Red Hat Advanced Cluster Security 4	A flaw was found in StackRox/RHACS Central's Auth Machine-to-Machine (M2M) token exchange. When an administrator configures M2M role mappings, the system uses unanchored regular expressions for matching claim values. This allows an attacker with a valid OpenID Connect (OIDC) token, whose claim value is a superstring of a configured pattern, to gain unauthorized access to roles they were not intended to receive. This can lead to privilege escalation within the system.	2026-08-10	6.8	CVE-2026-19278
Red Hat--Red Hat Advanced Cluster Security 4	A flaw was found in claircore's RPM package scanner. Crafted RPM header data in a container layer can cause an unchecked type assertion to panic the scanner. The panic is not recovered, causing the Clair indexer process to crash, leading to a denial of service.	2026-08-11	4.3	CVE-2026-19519
Red Hat--Red Hat Ansible	The 'podman quadlet install --replace' command opens the existing destination file with O_CREATE O_WRONLY but omits O_TRUNC. When the initial reflink copy	2026-08-13	4.2	CVE-2026-19730

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Automation Platform 2	attempt fails (common on non-reflink-capable filesystems including many RHEL default XFS configurations), the fallback in RefflinkOrCopy uses io.Copy which performs a non-truncating write. If the original Quadlet is larger than the new Quadlet, the file is not truncated and content from the original is preserved. The command completes with no warning. There is no risk of information leakage as the user already had access to the Quadlet in order to replace it, and in most cases, this would only lead to invalid Quadlet files. However, security-related options from the end of the old Quadlet could be included in the new Quadlet, and if the truncation resulted in a valid Quadlet file, this could result in undesirable behavior. For example, running podman quadlet install --replace to remove a single line from the end of a Quadlet - including security-sensitive content, like AddCapability - will fail, and the option will continue to be used. Further, with Volume Quadlets, this can include additional mounts which can cause content to be unintentionally exposed into containers. If, later, the image is updated then compromised content might be leaked to an attacker. The vulnerable code paths are in pkg/domain/infra/abi/quadlet.go (lines 338-360, O_CREATE O_WRONLY without O_TRUNC) and vendor/go.podman.io/storage/pkg/fileutils/reflink_linux.go (lines 12-19, non-truncating io.Copy fallback).			
Red Hat--Red Hat build of Apache Camel for Spring Boot 4	A flaw was found in the ChunkReader component of the Undertow HTTP server, which is used by WildFly and JBoss EAP to handle chunked transfer encoding. The issue occurs because the parser uses a single internal variable to store both the remaining chunk size and state flags. By sending a specially crafted request with an extremely large chunk size, an attacker can cause these values to overlap, tricking the parser into thinking a request has finished prematurely. This can allow a second, "smuggled" request to be processed out of sync, potentially bypassing security controls.	2026-08-11	5.3	CVE-2026-14180
Red Hat--Red Hat build of Apache Camel for Spring Boot 4	A flaw was found in Undertow, an HTTP server, within its HTTP response header writing path. The `writeString()` method performs a silent narrowing cast from 16-bit Unicode characters to 8-bit bytes when writing HTTP response header values. A remote attacker can exploit this by supplying specific Unicode characters in user-controlled input that an application places into response headers. This can lead to the truncation of these characters into ASCII control characters or special symbols, potentially resulting in limited integrity impact or information disclosure if the application does not properly sanitize user input.	2026-08-14	5.3	CVE-2026-19879
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. The CleanAllRUV and Abort CleanAllRUV replication-maintenance extended operations perform no authorization check, allowing an unauthenticated remote attacker to invoke them when nsslapd-allow-anonymous-access is enabled (the default), or any authenticated low-privilege user to invoke them otherwise. This allows removal of a replica ID from replication metadata, purging of changelog records, and interruption of administrator-initiated cleanup, which can leave replication inconsistent or unavailable.	2026-08-10	6.5	CVE-2026-19404
Red Hat--Red Hat Directory Server 11	A flaw was found in 389-ds-base. The get_ldapmessage_controls_ext() function frees the parsed controls array on the Session Tracking critical-control rejection path without clearing the SLAPI_REQCONTROLS pblock slot. Operation teardown then frees the same pointer again, causing a double-free. An unauthenticated remote attacker can trigger this with a single BIND request carrying a critical Session Tracking control, resulting in heap corruption and potential denial of service.	2026-08-12	5.9	CVE-2026-18663
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in open-iscsi. This vulnerability allows a remote attacker on the same local network segment to cause a Denial of Service (DoS) in the iscsiuid daemon. By sending a specially crafted Internet Control Message Protocol version 6 (ICMPv6) Router Advertisement with a zero-length option, the attacker can trigger an infinite loop. This leads to sustained CPU usage, rendering the daemon unresponsive and impacting system availability. A secondary risk of out-of-bounds	2026-08-12	6.5	CVE-2026-18726

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	reads exists with a short IPv6 payload, though no memory corruption or data exposure has been confirmed.			
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in open-iscsi's iscsiui component. This vulnerability involves an integer underflow and out-of-bounds read during Dynamic Host Configuration Protocol for IPv6 (DHCPv6) packet parsing. Specifically, crafted DHCPv6 Advertise traffic with a short User Datagram Protocol (UDP) length can cause the DHCPv6 payload length to underflow. An unauthenticated attacker on an adjacent network segment can exploit this by sending specially crafted IPv6 UDP traffic while the client is in an active DHCPv6 exchange, leading to a denial of service due to a process crash or service disruption.	2026-08-12	6.5	CVE-2026-18727
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in open-iscsi. An integer underflow vulnerability in the `iscsiui` component, specifically during IPv4 Dynamic Host Configuration Protocol (DHCP) parsing, allows a remote attacker on the same local network segment to cause a denial of service. By sending a specially crafted IPv4/UDP DHCP reply, the attacker can trigger an out-of-bounds read, leading to the `iscsiui` process crashing. This issue affects systems where `iscsiui` is actively handling IPv4 DHCP traffic.	2026-08-13	6.5	CVE-2026-18728
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in Samba's CTDB, the clustered database service used by Samba. Insufficient integrity validation of received CTDB protocol packets allows malformed packets containing invalid field lengths, improperly terminated strings, or inconsistent packet sizes to be processed without adequate bounds checking. A remote attacker with access to the CTDB private network may trigger a denial of service through process crashes or excessive memory consumption and, in limited cases, disclose adjacent memory contents.	2026-08-14	6.5	CVE-2026-58224
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in sblim-sfcb. A local attacker with access to the system can exploit an unsafe deserialization vulnerability in the provider-manager's inter-process communication (IPC) message parsing. By sending a specially crafted message, the attacker can cause out-of-bounds memory access, leading to the termination of the provider-manager process and a denial of service. This could also potentially result in limited unintended information disclosure.	2026-08-13	6.6	CVE-2026-73583
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in sblim-sfcb. A local, low-privileged attacker can exploit a race condition during privileged instance migration by manipulating a temporary file in the `/tmp` directory. By repeatedly recreating a symbolic link, the attacker can redirect privileged output to an arbitrary file. This can lead to privileged file corruption or a denial of service (DoS) on the system.	2026-08-13	6.3	CVE-2026-73584
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in sblim-cmpi-base. Insecure temporary file creation in the provider registration scripts allows a local unprivileged user to perform a symlink attack. By creating a symlink in a world-writable directory, an attacker can redirect privileged writes to an arbitrary file during script execution in a privileged context. This can lead to the overwrite of root-owned files, potentially disrupting system services or operation. Exploitation is conditional on the script running with elevated privileges and may be mitigated by sticky-directory symlink protections.	2026-08-13	6.3	CVE-2026-73585
Red Hat--Red Hat Enterprise Linux 10	Multiple Use-After-Free vulnerabilities were found in the add_archive_element function in ld/ldmain.c of the GNU linker (ld), a component of binutils. The root cause is that plugin_maybe_claim() in ld/plugin.c frees the original BFD object via bfd_close/_bfd_delete_bfd when entry->the_bfd->my_archive == NULL, but the caller retains both the original abfd parameter and a shallow copy (orig_input.the_bfd) as dangling pointers. These dangling pointers are subsequently dereferenced at three distinct locations in add_archive_element: 1. Line ~1442: accessing abfd->my_archive via bfd_usrdata(abfd->my_archive) 2. Line ~1493: multiple accesses to abfd and abfd->my_archive in a conditional check and bfd_get_filename call 3. Line ~1525: dereferencing the shallow copy orig_input.the_bfd->my_archive in trace/verbose logging The vulnerability is triggered when LTO plugins are active (link_info.lto_plugin_active is true) and the input object has abfd->my_archive == NULL, which is a valid state for standalone	2026-08-12	5.5	CVE-2026-19548

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	object files. Red Hat builds binutils with --enable-plugins and --enable-lto, confirming the vulnerable code path is compiled in and reachable. An attacker who can supply a crafted object or archive file to a build process using LTO-enabled linking could exploit this flaw to cause a denial of service (linker crash via segmentation fault). Arbitrary code execution is theoretically possible through heap manipulation but is substantially mitigated by hardening measures including stack protector, FORTIFY_SOURCE, ASLR, and PIE. The attack surface is limited to build-time environments - the linker is a development tool not exposed in production runtime. The most realistic exploitation scenario is a supply chain attack introducing a crafted object file as a build dependency in CI/CD pipelines or development environments.			
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in libdm. A local attacker could craft a malicious Logical Volume Manager (LVM) metadata configuration with deeply nested structures. This could lead to uncontrolled recursion in the libdm configuration file parser, exhausting the stack and causing any LVM command reading the metadata to crash. This vulnerability results in a Denial of Service (DoS) for affected systems.	2026-08-14	5.5	CVE-2026-19617
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in libvirt. During storage volume clone or convert operations, newly created volume images were temporarily world-readable. This was caused by the `qemu-img` utility running with overly permissive file creation settings, allowing any local user to read the full guest disk contents. This vulnerability could lead to sensitive information disclosure from guest virtual machines.	2026-08-10	5.5	CVE-2026-63623
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in iperf3. A remote unauthenticated attacker can exploit a vulnerability in the `JSON_read()` function, which accepts a peer-controlled message length and allocates memory without an upper bound. This allows the attacker to trigger excessive memory consumption, leading to a Denial of Service (DoS) through memory exhaustion, severe slowdown, or termination of the iperf3 service.	2026-08-11	5.3	CVE-2026-71218
Red Hat--Red Hat Enterprise Linux 10	A flow has been identified into dnsmsec library, causing an infinite loop to dnsmsec service. An attacker who controls any DNSSEC-signed zone can hang the dnsmsec process with a single crafted response, killing all DNS resolution for its clients.	2026-08-14	4.4	CVE-2026-13002
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in FreeIPA. The trust-fetch-domains command is gated by a read-only permission on the trust object rather than a trust-administration permission, allowing an authenticated, non-privileged IPA user to trigger a privileged Active Directory trust refresh using an attacker-supplied server and credentials, resulting in unauthorized, attacker-controlled modification of trusted-domain and ID-range identity data in the IPA LDAP directory.	2026-08-11	4.3	CVE-2026-19550
Red Hat--Red Hat Enterprise Linux 10	A type mismatch vulnerability was found in QEMU's vhost inflight migration VMState handling. The destination buffer size is stored as a uint64_t but read by the VMS_VBUFFER load path as a signed int32_t. On little-endian hosts, a crafted incoming migration state with bit 31 set causes the value to be interpreted as negative and then implicitly converted to a very large size_t, leading qemu_get_buffer() to copy migration-stream data beyond the bounds of the mmap-backed inflight region. This can result in a crash of the QEMU process or memory corruption. Exploitation requires control of the migration producer or write access to the migration channel, combined with a destination configured to use vhost inflight migration.	2026-08-10	4.4	CVE-2026-6426
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in GIMP. A signed integer overflow vulnerability exists in the `file-fli` plugin when processing FLI image files. This occurs due to an incorrect calculation during memory allocation for image buffers, where the multiplication of image width and height can exceed the maximum integer value. A remote attacker could exploit this by tricking a user into opening a specially crafted FLI file, leading to the application crashing and resulting in a denial of service.	2026-08-10	5.5	CVE-2026-59088

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Fuse 7	A flaw was found in wildfly-core. A remote attacker, authenticated as a 'deployer' account, can import and deploy a malicious archive file from an untrusted source. This is achieved by leveraging WildFly libraries to craft a Java project that allows an HTTP POST request to upload and deploy the malicious archive. This could lead to further exploitation, such as arbitrary file read vulnerabilities.	2026-08-11	6.5	CVE-2026-24330
Red Hat--Red Hat Fuse 7	A flaw was found in wildfly-core. A remote user authenticated as an administrative user can inject a malformed payload into the Inet Address field through the Management Model. This injection causes the server to crash and become unrecoverable, as the payload is written into the standalone.xml configuration file. Manual intervention is required to restore server operation, leading to a denial of service.	2026-08-11	4.9	CVE-2026-24329
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in the `odh-model-controller`. An authenticated user with permissions to create custom resources can exploit a vulnerability in the `loadSecret` function. This function improperly reads the Secret namespace from user-controlled input without validation. This allows an attacker to read sensitive API keys and cloud credentials from other namespaces, leading to information disclosure.	2026-08-10	6.5	CVE-2026-16456
Red Hat--Red Hat OpenShift AI 2.25	A flaw was found in the Feast operator. A malicious tenant could inject arbitrary code into their feature repository. This code would be executed by an automated process with elevated privileges, allowing the tenant to steal sensitive credentials. This could lead to a direct escalation of privileges, granting the tenant administrative control over the Kubernetes cluster.	2026-08-10	5.5	CVE-2026-18942
Red Hat--Red Hat OpenShift Container Platform 4	A flaw was found in the oauth-server component. This open redirect vulnerability occurs when the 'then' parameter in the grant approval handler is not properly validated. A remote attacker can craft a malicious URL that, when approved or denied by an authenticated user, redirects them to an attacker-controlled website. This could enable phishing attacks, potentially tricking users into revealing sensitive information.	2026-08-11	4.3	CVE-2026-19078
Red Hat--Red Hat OpenShift Update Service	A flaw was found in Red Hat Quay. When the SECURITY_SCANNER_V4_PSK (pre-shared key) is not set, a remote unauthenticated attacker can send POST requests to the security scanner notification endpoint. This allows the attacker to flood the notification queue and inject path traversal characters into Clair API URL paths. The primary consequence is worker resource exhaustion and blind path manipulation on the configured Clair host, potentially leading to a denial of service.	2026-08-14	6.5	CVE-2026-74243
Red Hat--Red Hat OpenShift Update Service	A flaw was found in Red Hat Quay's JWT (JSON Web Token) validation for federated robot accounts and single sign-on (SSO) authentication. Multiple issues related to audience verification and the enforcement of `azp` and `sub` claims were identified. These flaws could allow an attacker with a validly-signed token from the same identity provider to bypass configured security restrictions. This bypass could lead to unauthorized access by circumventing intended audience, subject, or authorized-client limitations.	2026-08-14	5.4	CVE-2026-74240
Red Hat--Red Hat OpenShift Update Service	A flaw was found in Red Hat Quay. An administrator of any repository, by knowing or guessing a target notification's Universally Unique Identifier (UUID), can read the notification configuration, including sensitive details like webhook URLs, Slack tokens, and email addresses. This vulnerability also allows them to trigger test notifications for another repository. This could lead to unauthorized information disclosure and potential misuse of notification services.	2026-08-14	5.3	CVE-2026-74242
Red Hat--Red Hat OpenShift Update Service	A flaw was found in Red Hat Quay's Stripe billing webhook handler. This vulnerability allows an unauthenticated attacker to forge billing events by sending crafted JSON requests to the `/webhooks/stripe` endpoint without validating the Stripe-Signature header. Successful exploitation can lead to the unauthorized resetting of a namespace's build quota to its maximum and trigger unsolicited billing emails to namespace administrators.	2026-08-14	5.9	CVE-2026-74244

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat OpenShift Update Service	A flaw was found in Red Hat Quay's exported logs feature. An unauthenticated attacker with a valid file ID could download exported action logs without proper authorization. While file IDs are complex, they can be intercepted from plaintext email or webhook callbacks. This vulnerability leads to information disclosure, potentially exposing sensitive data such as usernames, email addresses, IP addresses, and action-specific metadata.	2026-08-14	5.9	CVE-2026-74245
Red Hat--Red Hat OpenShift Update Service	A flaw was found in Red Hat Quay's external Lightweight Directory Access Protocol (LDAP) authentication handling. When an LDAP referral is returned during authentication, the system does not properly escape the username input. This allows an attacker to inject LDAP filter metacharacters, enabling user-existence oracle attacks at the referral Directory Name (DN). This could also potentially influence which DN is used for password binding in multi-domain Active Directory environments.	2026-08-14	4.8	CVE-2026-74241
Red Hat--Red Hat OpenShift Update Service	A flaw was found in Red Hat Quay. A user with FEATURE_BUILD_SUPPORT enabled and repository write access can exploit a Server-Side Request Forgery (SSRF) vulnerability within the build API. This allows the user to provide a malicious URL, causing the Quay builder to make requests to internal network addresses. Such an action could lead to the disclosure of sensitive internal information.	2026-08-14	4.2	CVE-2026-74247
regclient--regclient	regclient is a Docker and OCI Registry Client in Go. Prior to version 0.11.5, credentials for a registry may be inadvertently leaked to external servers. A prerequisite for this attack is a malicious registry server, a malicious blob store, or a registry that does not restrict the external URLs for foreign blobs. Version 0.11.5 fixes the issue.	2026-08-12	6.8	CVE-2026-49349
revolutbusiness--Revolut Gateway for WooCommerce	Unauthenticated Broken Access Control in Revolut Gateway for WooCommerce < 4.22.10 versions.	2026-08-13	5.3	CVE-2026-73353
RocketChat--Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 7.10.14, 8.0.8, 8.1.7, 8.2.7, 8.3.7, 8.4.5, 8.5.2, and 8.6.1, the stream-notify-user stream in the WebSocket protocol allows an authenticated user to write arbitrary notification bodies because the sender is not checked, and the client-side UI can create an ephemeral fake message in another user's currently open chat. This issue is fixed in versions 7.10.14, 8.0.8, 8.1.7, 8.2.7, 8.3.7, 8.4.5, 8.5.2, and 8.6.1.	2026-08-10	5.4	CVE-2026-72918
RocketChat--Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 7.10.14, 8.0.8, 8.1.7, 8.2.7, 8.3.7, 8.4.5, 8.5.2, and 8.6.1, the channels.convertToTeam REST endpoint allows an authenticated registered user with the create-team permission to convert an unrelated public channel by supplying channelName instead of channelId because the edit-room permission is checked only for channelId. This issue is fixed in versions 7.10.14, 8.0.8, 8.1.7, 8.2.7, 8.3.7, 8.4.5, 8.5.2, and 8.6.1.	2026-08-10	4.3	CVE-2026-72919
rockiger--ReactPress	Subscriber Broken Access Control in ReactPress <= 3.4.0 versions.	2026-08-13	6	CVE-2026-66455
RsyncProject--rsync	rsync before 3.5.0 contains a filter rule bypass vulnerability that allows authenticated clients to override module-level filter restrictions by supplying malicious --filter merge file directives. Attackers can inject client-side merge file directives during filter evaluation to introduce rules that supersede daemon module-level restrictions, gaining access to files the module filter was intended to exclude.	2026-08-13	6.5	CVE-2026-53786
RsyncProject--rsync	rsync before 3.5.0 contains a newline injection vulnerability in the name-converter uid/gid mapping interface that allows local attackers to forge protocol messages by creating user or group names containing newline characters. Attackers can inject malicious newline characters into names communicated over the pipe-based line-	2026-08-13	6.5	CVE-2026-53788

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	oriented protocol to cause the rsync daemon to process attacker-influenced data as legitimate protocol input, corrupting uid/gid mapping logic.			
RsyncProject--rsync	rsync before 3.5.0 contains an improper path handling vulnerability that allows a malicious sender to expand the scope of --delete operations beyond the intended destination subtree by sending a crafted file list that causes rsync to reclassify implied parent directory entries or treat synthetic paths as the transfer root. Attackers can exploit multiple variants including implied parent reclassification, synthetic root path construction, legacy protocol behavior below version 30, and non-directory root handling to cause the receiver to delete files outside the authorized destination directory.	2026-08-13	6.5	CVE-2026-53789
RsyncProject--rsync	rsync before 3.5.0 contains an out-of-bounds read vulnerability in the sender-side block matching logic that allows a malicious receiver to trigger memory access before the start of an allocated buffer by sending a crafted checksum block with a length of zero. Attackers can send a specially crafted checksum set containing a zero-length block to cause a negative offset calculation during delta computation, resulting in an out-of-bounds read of file data buffer memory on the sender side.	2026-08-13	6.5	CVE-2026-53792
RsyncProject--rsync	rsync before 3.5.0 contains a time-of-check to time-of-use (TOCTOU) race condition vulnerability in the non-daemon receiver's destination directory handling that allows an attacker who can manipulate destination path parent components to redirect file writes to unintended locations. Attackers can substitute a symlink for a component of the destination path between the path resolution and chdir() call, causing the receiver's working directory to be established outside the intended destination tree so that subsequent relative-path file writes land in unintended filesystem locations.	2026-08-13	6.3	CVE-2026-53796
RsyncProject--rsync	rsync before 3.5.0 contains a symlink race condition vulnerability that allows local attackers to cause rsync to apply arbitrary ACLs or extended attributes to unintended files by substituting a symlink at a predictable destination path between the file write and the subsequent acl_set_file() or lsetxattr() call. Attackers can exploit this timing window to redirect ACL and xattr application through a crafted symlink to files outside the intended destination tree, potentially granting elevated permissions and enabling local privilege escalation.	2026-08-13	6.3	CVE-2026-53799
RsyncProject--rsync	rsync 3.2.3 before 3.5.0 contains an out-of-bounds write in parse_size_arg() where the return value of snprintf() is used directly as an index into a .bss-segment array without bounds checking. When snprintf truncates the formatted size string, the return value equals the number of characters that would have been written including the truncated portion, and this value may exceed the array length. The subsequent indexed write targets memory outside the intended array bounds, corrupting .bss memory.	2026-08-13	6.5	CVE-2026-70457
RsyncProject--rsync	rsync 3.1.0 before 3.5.0 contains a signed integer overflow vulnerability in the I/O timeout implementation that allows attackers to permanently disable connection timeouts by injecting MSG_IO_TIMEOUT messages carrying non-positive (zero or negative) values. Attackers can craft malicious MSG_IO_TIMEOUT messages that cause the timeout variable to wrap to a non-positive value, preventing the timeout check from firing and enabling idle or stalled connections to hold daemon slots indefinitely, leading to resource exhaustion.	2026-08-13	6.5	CVE-2026-70462
RsyncProject--rsync	rsync before 3.5.0 contains a logic error in --max-alloc handling that allows a sender or configuration setting --max-alloc=0 to disable allocation sanity checks entirely rather than enforcing a zero-byte cap. Attackers can exploit this flaw to cause the receiver to attempt unbounded memory allocations for file list and data structures, potentially exhausting available memory and causing a denial of service.	2026-08-13	5.3	CVE-2026-53794
RsyncProject--rsync	rsync before 3.5.0 contains a privilege confusion vulnerability in the name-converter subprocess uid/gid mapping that allows local attackers to cause transferred files to be owned by root by influencing name-converter responses to	2026-08-13	5.3	CVE-2026-53798

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	return empty values. When the name-converter subprocess returns an empty response for a uid or gid lookup, rsync incorrectly interprets it as a successful resolution to uid/gid 0 (root) rather than a lookup failure, and if the name-converter also signals fake super-user status, rsync proceeds with root ownership assignments for transferred files.			
RsyncProject--rsync	rsync before 3.5.0 contains a symlink race condition vulnerability in the sender's directory scanning logic that allows attackers to cause the sender to enumerate and transfer files outside the module root's intended subtree. Attackers who can create or manipulate symlinks in a path component of the scanned tree can replace a symlink with a directory entry pointing outside the module root between the lstat() call and the subsequent opendir() call, exposing files beyond the intended root in both daemon-mode and non-daemon sender-side scanning.	2026-08-13	5.9	CVE-2026-53801
RsyncProject--rsync	rsync 3.0.0 before 3.5.0 contains a null pointer dereference vulnerability in the daemon child process that allows remote attackers to crash the daemon by sending a file list whose first entry is a dot entry not typed as a directory. The daemon dereferences the first file list entry as a directory structure pointer without verifying the entry type, resulting in an invalid or uninitialized pointer dereference that terminates the client connection.	2026-08-13	5.3	CVE-2026-70459
RsyncProject--rsync	rsync before 3.5.0 contains a symlink race condition vulnerability in the sender's source tree traversal that allows an attacker who can manipulate a parent directory of the source tree to redirect file reads to unintended paths. Attackers can atomically replace a parent directory component with a symlink pointing outside the source root between path resolution and file open operations to disclose file contents outside the intended transfer root.	2026-08-13	4.7	CVE-2026-53797
RsyncProject--rsync	rsync before 3.5.0 contains a symlink race condition vulnerability in the --remove-source-files feature that allows attackers with symlink creation access to cause arbitrary file deletion. Attackers can atomically substitute a symlink for a source file between transfer completion and the unlink() call, causing rsync to delete the symlink target rather than the intended source file.	2026-08-13	4.7	CVE-2026-53800
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. RustFS authorizes explicit versionId reads in GetObject, CopyObject sources, and UploadPartCopy sources with s3:GetObject instead of s3:GetObjectVersion, allowing principals without historical-version permission to disclose known historical object content. This issue is fixed in version 1.0.0-beta.11.	2026-08-12	6.5	CVE-2026-73265
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.12, RustFS handles FTPS MKD in FtpsDriver::mkd in crates/protocols/src/ftps/driver.rs by calling storage.create_bucket without authorize_operation for S3Action::CreateBucket, allowing authenticated FTPS users denied s3:CreateBucket to create buckets. This issue is fixed in version 1.0.0-beta.12.	2026-08-12	5.4	CVE-2026-73287
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. Prior to 1.0.0-beta.12, an anonymous ListObjectVersions request in rustfs/src/storage/access.rs that lacks a direct bucket-policy grant falls back to an s3:ListBucket check and returns before the policy_allowed path applies deny_anonymous_table_data_plane_if_needed and RestrictPublicBuckets, so a bucket that permits anonymous listing can continue exposing version listings after an operator enables the public-access control. The bypass affects GET /<bucket>?versions= and can disclose object version metadata even though equivalent GetObject requests are denied. This issue is fixed in version 1.0.0-beta.12.	2026-08-12	5.3	CVE-2026-73290
s9y--Serendipity	Serendipity versions >= 2.3.5 and <= 2.6.0 contain a reflected cross-site scripting vulnerability in the search clean-URL route (/search/<term>). In include/functions_routing.inc.php serveSearch(), the sanitisation pipeline runs urldecode() after HTML-encoding, so a single URL-encoded HTML payload survives strip_tags() and htmlspecialchars() and is then decoded back into live HTML in the	2026-08-13	6.1	CVE-2026-73628

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	page. A crafted search link can execute arbitrary JavaScript in the victim's browser. Fixed in 2.6.1.			
saadiqbal--Advanced File Manager Ultimate File Manager for WordPress And Document Library Solution	The Advanced File Manager - Ultimate File Manager for WordPress And Document Library Solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'soundFile' parameter in all versions up to, and including, 5.4.12 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the attacker to control a domain whose origin string is a leading prefix of the target site's backend URL (e.g. https://example.co against https://example.com), and the victim must be an authenticated WordPress administrator who visits the attacker-controlled page while the File Manager admin screen is open.	2026-08-16	6.1	CVE-2026-15009
saithink--SaiAdmin	A security vulnerability has been detected in saithink/saigroup SaiAdmin up to 5.0.1. This impacts the function shell_exec of the file /app/saipackage/install/upload of the component Plugin Upload Endpoint. The manipulation leads to unrestricted upload. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This product is published by multiple vendors.	2026-08-10	4.7	CVE-2026-19383
Samsung Open Source--rlottie	Improper Validation of Specified Quantity in Input and Allocation of Resources Without Limits or Throttling vulnerability in Samsung Open Source rlottie allows Excessive Allocation.	2026-08-11	6.5	CVE-2026-19517
Samsung Open Source--rlottie	Improper Validation of Specified Quantity in Input vulnerability in Samsung Open Source rlottie allows Input Data Manipulation.	2026-08-11	6.5	CVE-2026-19518
Samsung Open Source--rlottie	Uncontrolled Resource Consumption vulnerability in Samsung Open Source rlottie allows Excessive Allocation.	2026-08-12	6.5	CVE-2026-19587
Samsung Open Source--rlottie	Integer Overflow to Buffer Overflow vulnerability in Samsung Open Source rlottie allows Overflow Buffers.	2026-08-12	6.5	CVE-2026-19588
SAP_SE--Odata	A malicious or compromised OData service could disclose sensitive authentication information and inject untrusted data into the application, which may leads to a high impact on confidentiality and low impact on integrity and no impact on Availability.	2026-08-11	5.9	CVE-2026-66773
SAP_SE--SAP ABAP Platform	SAP ABAP Platform allows an unauthenticated user to send a specially crafted request to an internal component. This could disclose limited, non-sensitive data from previously used memory, leading to a low on confidentiality, with no impact on integrity and availability of the application.	2026-08-11	5.3	CVE-2026-58247
SAP_SE--SAP Business AI Platform (Approuter)	SAP Approuter does not correctly validate client certificates in certain callback flows. An attacker with low privileges, holding a certificate from the same trusted authority with matching subject values, could bypass the identity check. This complexity makes the attack difficult to execute. Successful exploitation could allow impersonation of a trusted internal component, resulting in a high impact on integrity and a low impact on confidentiality and availability.	2026-08-11	6.4	CVE-2026-66760
SAP_SE--SAP Business AI Platform (Approuter)	WebSocket of SAP Approuter does not perform sufficient authorization checks in certain functionality. An attacker with low privileges could exploit this to access restricted functionality. Successful exploitation could allow the attacker to read sensitive information and perform limited modifications, resulting in a high impact on confidentiality and a low impact on integrity. There is no impact on availability.	2026-08-11	5.9	CVE-2026-58237
SAP_SE--SAP Business AI Platform (Approuter)	SAP Approuter does not sufficiently handle certain requests under specific conditions. An unauthenticated attacker could send specially crafted input that causes the component to crash and restart. Successful exploitation requires specific runtime conditions to be met, making the attack complex to execute. This	2026-08-11	5.9	CVE-2026-58238

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	results in a high impact on availability. There is no impact on confidentiality and integrity.			
SAP_SE--SAP Business AI Platform (Approuter)	SAP Approuter does not consistently enforce integrity verification on certain session-related request headers under specific conditions. An attacker with low privileges could send a specially crafted request that bypasses the integrity check and loads another user's session context. Successful exploitation requires the attacker to have previously observed matching session values out-of-band, which makes the attack complex to execute. This could result in a high impact on confidentiality and a low impact on integrity. There is no impact on availability.	2026-08-11	5.9	CVE-2026-66776
SAP_SE--SAP Business AI Platform (Approuter)	SAP Approuter does not sufficiently validate certain incoming requests before forwarding them to backend destinations. Due to the complexity of the required conditions, an attacker with low privileges could send specially crafted requests to bypass authorization checks and reach protected resources beyond their assigned scope. Successful exploitation could allow the attacker to read sensitive data and perform limited modifications on protected resources, resulting in a high impact on confidentiality and a low impact on integrity. There is no impact on availability.	2026-08-11	5.9	CVE-2026-66777
SAP_SE--SAP Business AI Platform (Approuter)	SAP Approuter does not sufficiently sanitize certain request headers before forwarding traffic to internal components. An unauthenticated attacker could send a specially crafted request to obtain limited unauthorized access to information. This results in a low impact on confidentiality. There is no impact on integrity and availability.	2026-08-11	5.3	CVE-2026-66778
SAP_SE--SAP Business AI Platform (Approuter)	SAP Approuter does not enforce sufficient flow control in certain functionality. An attacker with low privileges could send high volumes of data without consuming responses, causing unbounded memory growth. This results in a low impact on availability. There is no impact on confidentiality and integrity.	2026-08-11	4.3	CVE-2026-66761
SAP_SE--SAP Business AI Platform (Approuter)	SAP Approuter does not enforce cross-site request forgery protection on the authentication flow by default. An unauthenticated attacker could craft a malicious link and trick a victim into following it. Successful exploitation could allow the attacker to bind the victim's session to an attacker-controlled identity, resulting in a low impact on integrity. There is no impact on confidentiality and availability.	2026-08-11	4.3	CVE-2026-66775
SAP_SE--SAP BusinessObjects Business Intelligence	SAP BusinessObjects Business Intelligence Platform (Web Intelligence) allows a low-privileged attacker to upload a specially crafted spreadsheet file containing malicious external references. When the file is processed as a data source, the affected component resolves these references and exposes the contents of sensitive server-side files within the resulting report. This results in a high impact on confidentiality, with no impact on integrity and availability.	2026-08-11	6.5	CVE-2026-58248
SAP_SE--SAP BusinessObjects Business Intelligence Platform (Admin Tools)	SAP BusinessObjects Business Intelligence Platform (Admin Tools) does not perform sufficient authorization check on certain administrative functionality. An attacker authenticated as a non-administrative user could bypass this restriction to gain limited information about affected functionality. This results in a low impact on confidentiality. There is no impact on integrity and availability.	2026-08-11	4.3	CVE-2026-66772
SAP_SE--SAP Manufacturing Integration and Intelligence	SAP Manufacturing Integration and Intelligence (MII) does not perform necessary authorization check on certain application function, allowing a low-privileged authenticated attacker to access information that should be restricted to privileged users. Successful exploitation could allow the attacker to access the users account information in the application, which could be leveraged to facilitate further attacks against the identified user accounts. This vulnerability results in low impact on confidentiality of the data, with no impact on the integrity and availability	2026-08-11	4.3	CVE-2026-58244
SAP_SE--SAP NetWeaver and ABAP Platform (Change and	SAP NetWeaver and ABAP Platform (Change and Transport System - Customer Transport Integration Wizard) allows a low-privileged user to modify configuration tables that control access to data objects during specific operations. These unauthorized modifications could result in processing delays and operational	2026-08-11	4.2	CVE-2026-58241

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Transport System - Customer Transport Integration Wizard	disruption, leading to a low impact on the integrity and availability of the application with no impact on confidentiality.			
SAP_SE--SAP NetWeaver Application Server ABAP	Due to a Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Application Server ABAP, an authenticated attacker could generate a malicious link and make it publicly accessible. If an authenticated victim accesses this link, the injected input is processed and reflected within the DOM on the client side during page rendering, resulting in the execution of malicious content in the victim's browser context. Successful exploitation could result in a high impact to the confidentiality and a low impact to the integrity of the system, while availability remains unaffected.	2026-08-11	6.3	CVE-2026-66779
SAP_SE--SAP NetWeaver Application Server ABAP and ABAP Platform	SAP NetWeaver Application Server ABAP and ABAP Platform allow an attacker with high privileges to bypass missing security controls on an internal code path leading to operating system command execution. Successful exploitation could allow the attacker to execute OS-level commands that write to the operating system or stop the SAP system, resulting in no impact on confidentiality, low impact on integrity, and high impact on availability.	2026-08-11	5.5	CVE-2026-58236
SAP_SE--SAP NetWeaver AS Java (Adobe Document Services)	SAP NetWeaver Application Server Java (Adobe Document Service) uses outdated open source cryptographic and data transfer libraries that contain known vulnerabilities addressed in later versions. A low-privileged authenticated attacker could potentially leverage these weaknesses against the affected component, though no specific exploit is currently known. Successful exploitation could result in low impact on confidentiality, integrity, and availability of the system.	2026-08-11	6.3	CVE-2026-58235
SAP_SE--SAP S/4 HANA (Reprocess Bank Statement Items)	Reprocess Bank Statement Items in SAP S/4HANA does not perform the necessary authorization checks for authenticated users, allowing them to use rules that have not been shared with them, resulting in privilege escalation. This vulnerability has a low impact on confidentiality, with no impact on integrity and availability of the application	2026-08-11	4.3	CVE-2026-66764
SAP_SE--SAP Social Intelligence	Due to an SQL Injection vulnerability in SAP Social intelligence, an authenticated attacker could directly inject an SQL DDL (Data Definition Language) string into the underlying database without further authorization. Successful exploitation could allow the attacker to make malicious changes to the database structure, resulting in a low impact to the confidentiality, integrity, and availability of the system.	2026-08-11	6.3	CVE-2026-66770
SAP_SE--SAPSPrint Service	SAP SAPSPrint Service has memory corruption vulnerabilities in the handling of certain commands. An unauthenticated attacker could send specially crafted requests that trigger a buffer overflow in the affected component. This causes a temporary service interruption and automatic restart, resulting in low impact on availability but no impact on confidentiality and integrity.	2026-08-11	5.3	CVE-2026-40130
SAP_SE--SAPUI5	SAPUI5 allows a key user with content adaptation privileges to inject malicious script content into persisted application changes. When another user subsequently opens the adapted application, the injected script executes in the victim's browser session. Successful exploitation could allow the attacker to access sensitive session data and perform unauthorized actions on behalf of the victim, resulting in a high impact on confidentiality and integrity. There is no impact on availability.	2026-08-11	6.1	CVE-2026-66771
Saurus--Saurus CMS Community Edition	Saurus CMS Community Edition contains an unauthenticated open redirect vulnerability in the logout handling code in classes/port.inc.php, where the url parameter supplied via GET or POST is passed directly to the Location header without domain allowlist, scheme validation, or relative path enforcement. Attackers can craft a malicious logout URL containing an arbitrary external domain or javascript: URI scheme to redirect authenticated users to attacker-controlled phishing pages after session destruction, enabling credential theft and OAuth redirect abuse.	2026-08-13	6.1	CVE-2026-73671

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SCADA-LTS-- ScadaLTS	ScadaLTS 2.7.8.1 reflects user-supplied input into an HTML response without sanitization. An unauthenticated attacker who lures a victim into visiting a crafted URL can execute arbitrary JavaScript in the context of the victim's browser session.	2026-08-12	6.1	CVE-2026-19657
Scott Paterson-- Contact Form 7 PayPal & Stripe Add-on	Unauthenticated Broken Access Control in Contact Form 7 - PayPal & Stripe Add-on <= 2.5.1 versions.	2026-08-13	6.5	CVE-2026-66660
scriban--scriban	Scriban before 7.0.0 contains three distinct denial-of-service vulnerabilities in expression evaluation that bypass existing safety controls through unbounded string multiplication, uncontrolled BigInteger shift operations, and LoopLimit bypass via range enumeration in builtin functions. Attackers who can supply templates can cause out-of-memory exceptions or CPU exhaustion, typically terminating the entire host process.	2026-08-16	6.5	CVE-2026-74785
scriban--scriban	Scriban before 7.0.0 (affected versions <= 6.6.0) contains a denial-of-service vulnerability in which the LimitToString safety limit (default 1MB) can be bypassed because ObjectToString resets the per-call length counter (_currentToStringLength) on every top-level call and StringBuilderOutput enforces no cumulative output-size limit. An attacker who can supply a template can render a near-limit string repeatedly in a loop, allocating approximately 1GB of memory and causing an out-of-memory condition that crashes the host application.	2026-08-16	6.5	CVE-2026-74786
shortpixel-- ShortPixel Adaptive Images WebP, AVIF, CDN, Image Optimization	The ShortPixel Adaptive Images - WebP, AVIF, CDN, Image Optimization plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.11.5. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify configuration options of third-party plugins including ShortPixel Image Optimizer, Autoptimize, WP Rocket, Imagify, and LiteSpeed Cache, as well as the plugin's own API key and account binding. Exploitation requires the respective third-party plugins to be installed, as the impact against those plugins' settings is only reachable when those plugins are present.	2026-08-16	4.3	CVE-2026-15345
Siemens--Desigo DXR2	A vulnerability has been identified in Desigo DXR2 (All versions < V01.21.233.16-7862), Desigo PXC3 (All versions < V01.21.233.16-7862), Desigo PXC4 (All versions < V02.21.194.36-2715), Desigo PXC5.E003 (All versions < V02.21.194.36-2715), Desigo PXC5.E24 (All versions < V02.21.194.36-2715), Desigo PXC7 (All versions < V02.21.194.36-2715). The affected devices are vulnerable to a denial-of-service (DoS) vulnerability. An attacker can exploit this issue by sending a malformed BACnet packet, causing the device to stop responding to BACnet queries. Recovery requires a device reset or reboot to restore normal functionality.	2026-08-11	4.3	CVE-2026-59693
Siemens--LOGO! Soft Comfort	A vulnerability has been identified in LOGO! Soft Comfort (All versions < V9). Affected products use a static, hardcoded AES master key to encrypt project files. This could allow a local attacker to extract the master key from the application files or memory and use it to decrypt project files or remove project passwords entirely without knowing the actual user-defined password.	2026-08-11	6.8	CVE-2026-57262
Siemens--LOGO! Soft Comfort	A vulnerability has been identified in LOGO! Soft Comfort (All versions < V9). The project password feature in the affected products stores the password as an unsalted SHA-256 hash. This could allow an attacker who has obtained the project file to perform efficient offline dictionary or brute-force attacks against the unsalted hash.	2026-08-11	6.8	CVE-2026-57263
Siemens--Siemens License Server (SLS)	A vulnerability has been identified in Siemens License Server (SLS) (All versions < V5.1). The affected application is vulnerable to a local privilege escalation due to an insecure sudoers policy. This could allow an attacker to execute arbitrary commands and plant malicious files as root, leading to full system compromise.	2026-08-11	6	CVE-2026-69108

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Signify--Philips Hue Bridge Pro	The Signify Philips Hue Bridge Pro firmware embeds a Mosquitto MQTT broker (v2.0.22) that listens on all network interfaces with anonymous access enabled and no firewall restriction. An attacker with access to the Bridge's network can read device data and control connected lights.	2026-08-13	6.3	CVE-2026-73669
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain a missing authorization vulnerability in the /api/ref/refreshBacklink endpoint that allows anonymous readers to trigger persistent server-side writes. Attackers can invoke the endpoint with an attacker-controlled block ID to flush transaction queues, scan all references globally, and enqueue database writes, bypassing read-only protections and enabling resource amplification attacks.	2026-08-14	6.5	CVE-2026-72812
siyuan-note--siyuan	siyuan versions <= 3.7.3 (fixed in v3.7.4) contain a server-side template injection vulnerability in the attribute-view Template calculation feature (introduced in v3.7.0-beta.1). The feature's template engine uses Sprig's unmodified function map, which still exposes the env, expandenv, and getHostByName functions that were removed elsewhere for CVE-2024-55660. A local, unauthenticated attacker (the kernel binds to 127.0.0.1 by default with no per-UID access control) can inject a malicious Template calculation formula to read environment variables belonging to the account running siyuan - including from a separate, unprivileged OS account - and to perform DNS lookups from the server's network position.	2026-08-15	6.2	CVE-2026-73047
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an information disclosure vulnerability in the UILayout filter that fails to properly restrict administrator workspace state from publish readers. Unauthenticated attackers can retrieve the administrator's open documents, search terms, notebook paths, and private asset locations by calling the getConf endpoint without authentication.	2026-08-12	5.8	CVE-2026-72788
siyuan-note--siyuan	SiYuan before v3.7.4 contains an information disclosure vulnerability in the /api/notebook/getNotebookInfo endpoint that returns notebook metadata without authorization checks. Attackers can read notebook names, document counts, sizes, and timestamps for closed or non-published notebooks that should be hidden from readers.	2026-08-12	5.8	CVE-2026-72790
siyuan-note--siyuan	SiYuan v3.7.4-alpha.1 (a pre-release; the endpoint does not exist in stable v3.7.3 or earlier) contains an information disclosure vulnerability in the /api/av/getAttributeFieldViews endpoint. The route is registered with CheckAuth only and applies no publish-access filtering, so reader-role callers can retrieve the complete database view structure - every view's name, icon, layout type, and per-field Hidden flag - for any database whose avID is supplied, regardless of authorization. The issue was introduced by commit acfc02ee8 and fixed in v3.7.4.	2026-08-12	5.8	CVE-2026-72791
siyuan-note--siyuan	SiYuan before v3.7.4 contains an information disclosure vulnerability in the /api/tag/getTag endpoint that returns tag labels and occurrence counts from password-protected documents to unauthenticated readers. Attackers can enumerate tag vocabulary and internal terminology from password-protected documents by calling the tag endpoint without providing the document's publish password.	2026-08-12	5.8	CVE-2026-72792
siyuan-note--siyuan	SiYuan before v3.7.4 contains an access control bypass vulnerability where static-file routes in the server mux bypass publish-access controls enforced on the REST API. Attackers with publish reader tokens or anonymous access in disabled-auth mode can read templates, snippets, and export artifacts by directly accessing static routes that lack the same restrictions as their REST API counterparts.	2026-08-12	5.8	CVE-2026-72796
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an information disclosure vulnerability in the getEncryptedNotebookStatus endpoint that returns encrypted notebook identifiers, names, and lock states without publish-access filtering. Anonymous readers and publish-mode accounts can enumerate all encrypted notebooks and	2026-08-12	5.8	CVE-2026-72797

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	their current unlock status, revealing sensitive notebook names and decryption state in memory.			
siyuan-note--siyuan	SiYuan before v3.7.4 (affected <=v3.7.2) fails to enforce publish-access filters on five filetree path-resolution endpoints (getFullHPathByID, getHPathByID, getPathByID, getIDsByHPath, and getHPathByPath). In publish mode, when Publish.Auth.Enable is false, an unauthenticated (anonymous) reader - or any publish reader token - can call these endpoints to enumerate the complete private document tree, mapping notebook names, folder hierarchies, and document titles, and resolving title paths to document IDs, including for documents marked hidden, password-protected, or publish-forbidden.	2026-08-12	5.8	CVE-2026-72799
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to apply publish-access filtering to the getAttributeViewKeysByID endpoint, allowing authenticated readers to retrieve complete database column schemas including descriptions, select vocabularies, and template expressions. Additionally, getBlockDefIDsByRefText and getBlockRelevantIDs endpoints enumerate workspace-wide block IDs without publish scoping, enabling attackers to discover valid block identifiers across publish boundaries and access content from hidden or password-protected documents.	2026-08-12	5.8	CVE-2026-72800
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an information disclosure vulnerability in the resolveAssetPath endpoint that returns absolute filesystem paths unmodified to CheckAuth-only requests. Attackers can harvest relative asset paths from published documents and submit them to resolveAssetPath to obtain the server's absolute workspace path, disclosing the operating-system username and installation layout.	2026-08-12	5.3	CVE-2026-72802
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to enforce publish-access checks in the getBlockAttrs and batchGetBlockAttrs endpoints. Attackers can retrieve block attributes including names, aliases, memos, and custom fields from protected documents by sending POST requests with block IDs.	2026-08-12	5.8	CVE-2026-72803
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to enforce publish-access checks on getBlockBreadcrumb, getRefText, and getBlockTreeInfos endpoints, allowing disclosure of protected document content and metadata. Anonymous readers or publish RoleReader accounts can retrieve document titles, ancestor block content snippets, reference text, and path metadata for publish-forbidden or password-protected documents by supplying block IDs.	2026-08-12	5.8	CVE-2026-72805
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an authentication bypass vulnerability in the FilterViewByPublishAccess filter that fails to check publish password protection when rendering attribute views and database rows. Unauthenticated readers can access password-protected document rows including titles, block IDs, and column values by calling renderAttributeView without supplying the required password.	2026-08-12	5.8	CVE-2026-72806
siyuan-note--siyuan	SiYuan versions up to and including v3.7.2 (fixed in v3.7.4) contain an information disclosure vulnerability in the /api/asset/getFileAnnotation endpoint, which returns .sya PDF-annotation file content without a publish-access check. Because the endpoint is gated only by CheckAuth (unlike the /assets/* route, which enforces publish access and password), an anonymous reader (when publish authentication is disabled) or any publish RoleReader who knows an asset path can read the private PDF annotations (highlights and notes) of publish-forbidden, password-protected, or unpublished documents. The issue is limited to non-encrypted notebooks; encrypted-box annotations are not exposed.	2026-08-12	5.8	CVE-2026-72808
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an information disclosure vulnerability in the getRefIDsByFileAnnotationID endpoint that returns block identifiers citing PDF annotations without publish-access filtering. Attackers can extract block identifiers from restricted documents by supplying annotation identifiers visible in published pages, revealing citation relationships across forbidden and password-protected tiers.	2026-08-14	5.8	CVE-2026-73048

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an information disclosure vulnerability in the <code>getAttributeViewBacklinks</code> endpoint that consults the forbidden access list instead of the visibility list when filtering backlinks. Anonymous readers can supply a publicly visible database row identifier to discover hidden-tier documents that reference it, receiving the database name, row title, and document path of hidden documents.	2026-08-14	5.8	CVE-2026-73049
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain a path traversal vulnerability in the <code>getUniqueFilename</code> endpoint that allows anonymous readers to probe filesystem existence without validation or confinement. Attackers can supply arbitrary absolute paths to determine whether files and directories exist on the host, enabling reconnaissance of the filesystem layout and installed software.	2026-08-13	5.8	CVE-2026-73605
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an information disclosure vulnerability in the <code>/api/block/getRefIDs</code> endpoint that fails to check password-protected document tiers. Unauthenticated readers can discover that password-protected documents reference specific blocks and obtain block identifiers without entering the document password.	2026-08-13	5.8	CVE-2026-73606
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an information disclosure vulnerability in the <code>/api/storage/getOutlineStorage</code> endpoint that performs no authorization checks. Attackers can retrieve outline state including heading identifiers for any document by supplying its identifier, even for documents forbidden to the requester.	2026-08-13	5.8	CVE-2026-73607
siyuan-note--siyuan	SiYuan versions before v3.7.4 contain an information disclosure vulnerability in the <code>getBookmarkLabels</code> endpoint that returns all bookmark labels in the workspace without publish-access filtering. Anonymous readers and publish-mode readers can obtain the complete bookmark vocabulary across the workspace, disclosing subject matter and organizational information from inaccessible documents.	2026-08-13	5.8	CVE-2026-73609
siyuan-note--siyuan	SiYuan before v3.7.4 contains an information disclosure vulnerability in the local storage filter that returns the administrator's entire storage map with only three keys sanitized. Unauthenticated attackers or publish readers can retrieve closed-tab history, search keywords, private document identifiers, and expanded folder paths by calling the <code>getLocalStorage</code> endpoint.	2026-08-13	5.8	CVE-2026-73610
siyuan-note--siyuan	SiYuan before v3.7.4 contains an information disclosure vulnerability in the <code>/api/filetree/authFilePublishAccess</code> endpoint, which is registered with <code>CheckAuth</code> only and is reachable anonymously. The endpoint never sets a failure code, so its outcome is signalled entirely by the response message and by the presence of a <code>Set-Cookie</code> header, and these signals differ across access tiers. By submitting requests with an empty password for a candidate document identifier, an anonymous attacker can distinguish whether a document is public/nonexistent, password-protected, or exists at the hidden or forbidden tier, thereby confirming the existence of documents they are not permitted to access. Because hidden and forbidden entries store an empty password, such requests also cause the server to issue a publish-auth cookie for forbidden documents.	2026-08-14	5.8	CVE-2026-73630
smub--Smash Balloon Social Post Feed Simple Social Feeds for WordPress	The Smash Balloon Social Post Feed - Simple Social Feeds for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'id' Shortcode Attribute in all versions up to, and including, 4.9.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-16	6.4	CVE-2026-16775
SourceCodester--Air Cargo Management System	A vulnerability was determined in SourceCodester Air Cargo Management System 1.0. Impacted is an unknown function of the file <code>/classes/Master.php?f=save_cargo_type</code> . Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-14	4.7	CVE-2026-19787

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Online Clothing Store	A vulnerability has been found in SourceCodester Online Clothing Store 1.0. This affects an unknown part of the file /db/shopping.sql of the component SQL Database Backup. The manipulation leads to files or directories accessible. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2026-08-15	5.3	CVE-2026-19903
SourceCodester--Simple Doctors Appointment System	A vulnerability was detected in SourceCodester Simple Doctors Appointment System 1.0. This issue affects the function save_doctor of the file /save_file.php. The manipulation results in unrestricted upload. The attack can be executed remotely. The exploit is now public and may be used.	2026-08-14	4.7	CVE-2026-19839
SourceCodester--Stock Management System	A vulnerability was detected in SourceCodester Stock Management System 1.0. This issue affects some unknown processing of the file /classes/Master.php?f=delete_supplier. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	2026-08-16	4.7	CVE-2026-19925
Space Codes--AI for SEO	Unauthenticated Broken Access Control in AI for SEO <= 2.4.2 versions.	2026-08-13	6.5	CVE-2026-66459
Spacebar Server--Spacebar Server	Spacebar Server before commit 8d126f4 contains a cross-channel message deletion vulnerability in the single-delete and bulk-delete message handlers that fail to scope message queries to the requested channel. Authenticated users with MANAGE_MESSAGES permission in any controlled channel can delete arbitrary messages in other channels by routing delete requests through their own channel.	2026-08-10	6.5	CVE-2026-69114
SpaceX--Starlink Router Gen 3	A vulnerability has been found in SpaceX Starlink Router Gen 3 2025.11.14.mr64708.3. This affects the function get_status of the component gRPC Management Interface. The manipulation leads to improper access controls. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-15	6.3	CVE-2026-19918
squidfunk--mkdocs-material	Material for MkDocs is a powerful documentation framework built on top of MkDocs. From 7.2.0 until 9.7.7, the mountSearchSuggest function in src/templates/assets/javascripts/components/search/suggest/index.ts contains a DOM-based cross-site scripting vulnerability in the optional search.suggest feature that allows a crafted q URL parameter to execute JavaScript in a documentation site's origin after user interaction. This issue is fixed in version 9.7.7.	2026-08-12	5.4	CVE-2026-73295
stoatchat--stoatchat	stoatchat before 0.15.0 contains a permission bypass vulnerability in the message_fetch route that checks only ViewChannel permission instead of requiring ReadMessageHistory. Attackers with ViewChannel access but ReadMessageHistory denied can retrieve individual message content by ID, bypassing the intended history restriction enforced by bulk read routes.	2026-08-16	6.5	CVE-2026-73059
stoatchat--stoatchat	stoatchat versions before 0.15.0 fail to block the IPv6 unspecified address (::) in the SSRF blocklist, allowing unauthenticated attackers to bypass protections via the /proxy and /embed endpoints. Attackers can craft requests using IPv6 literal syntax to access services on the loopback interface and retrieve sensitive internal content.	2026-08-16	5.8	CVE-2026-73058
streamaserver--streama	streama contains an insecure direct object reference vulnerability in ViewingStatusController that allows authenticated users to read and delete other users' viewing status records. Attackers can enumerate all users' watch progress, delete arbitrary viewing history, and manipulate other users' Continue Watching dashboards by supplying arbitrary primary keys without ownership verification.	2026-08-13	5.4	CVE-2026-73039
Stylemix--Motors	Subscriber Broken Access Control in Motors <= 1.4.113 versions.	2026-08-13	6.5	CVE-2026-66693
Sucuri--sucuri-wordpress-plugin	Sucuri Security WordPress plugin through version 2.7.3 contains a path traversal vulnerability in the pageIntegritySubmission() method in src/integrity.lib.php that allows authenticated administrators to delete arbitrary files by supplying directory	2026-08-10	6.5	CVE-2026-73033

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	traversal sequences in the <code>sucuriscan_integrity</code> parameter. Attackers can manipulate the unsanitized file path concatenated with <code>ABSPATH</code> to traverse outside the WordPress installation directory and invoke <code>unlink()</code> on sensitive files such as <code>wp-config.php</code> and <code>.htaccess</code> , causing site outage or enabling malicious reinstallation.			
sunnyadn--js-toml	js-toml is a TOML parser for JavaScript. Prior to version 1.1.2, the interpreter checks whether a key already exists in a parser-built container with <code>`if (object[key])`</code> instead of <code>`if (key in object)`</code> . When the prior value is a falsy primitive - <code>`false`</code> , <code>`0`</code> , <code>`0n`</code> , <code>`0.0`</code> , <code>`-0`</code> , or <code>`""`</code> - the duplicate-key branch is skipped and the value is silently overwritten by a later sub-table, dotted-key sub-table, or array-of-tables sharing the same name. Per the TOML 1.0.0 spec ("Defining a key multiple times is invalid"; "You cannot define any key or table more than once"), this should be a parse error. The result is structural type confusion of attacker-named keys in the value returned by <code>`load()`</code> . A boolean-typed <code>`false`</code> (or numeric <code>`0`</code>) becomes a truthy object. Host applications that gate behavior on <code>`if (config.flag)`</code> , <code>`if (!user.banned)`</code> , <code>`if (config.allowDelete)`</code> , or <code>`if (config.publicMode)`</code> will silently take the truthy branch. This is distinct from GHSA-65fc-cr5f-v7r2 (the 1.0.2 prototype-pollution fix). <code>`Object.prototype`</code> is not polluted. The <code>`Object.create(null)`</code> mitigation from 1.0.2 is intact; the bug here is in the duplicate-key state machine, not in container construction. Version 1.1.2 patches the incorrect comparison.	2026-08-14	5.3	CVE-2026-50029
supsysitic--Popup by Supsysitic	Unauthenticated Cross Site Scripting (XSS) in Popup by Supsysitic <= 1.11.2 versions.	2026-08-13	6.5	CVE-2026-27537
swc-project--swc	SWC is a TypeScript / JavaScript compiler written in Rust. Prior to @swc/html 1.15.47-nightly-20260729.1 and swc_html_minifier 59.0.0, the minifyJson processing in <code>crates/swc_html_minifier/src/lib.rs</code> parsed and serialized attacker-controlled JSON in <code>application/json</code> and <code>application/ld+json</code> script elements without the <code>escape_json_for_html_script</code> behavior to re-escape less-than signs, allowing a closing script sequence to terminate the element early and execute script in the generated page's origin. This issue is fixed in @swc/html 1.15.47-nightly-20260729.1 and swc_html_minifier 59.0.0.	2026-08-11	6.1	CVE-2026-72925
systemd--systemd-homed	systemd-homed contains a local privilege escalation bug via arbitrary system group addition to a local, logged in, homed-managed user	2026-08-10	6.7	CVE-2026-16742
systemd--systemd-machined	When systemd-machined >= v259 (or v258 with a custom <code>`polkit`</code> policy that allows <code>`register-machine`</code> access) is running on a desktop system, an unprivileged user logged in a desktop graphical session can kill arbitrary processes, even privileged ones. - versions older than v259 are not affected, unless unprivileged access is granted for the <code>`register-machine`</code> polkit action via a local, custom policy config file - versions older than v258 are not affected - unrelated to the systemd service manager (pid 1 or user session managers) - systemd-machined is not typically installed by default, and is typically in an optional, separate package (e.g.: systemd-container) - terminal-only or remote sessions (e.g.: ssh) are not affected	2026-08-10	4.7	CVE-2026-15060
systemd--systemd-oomd	Local unprivileged users can terminate arbitrary local processes via a systemd-oomd IPC API due to a missing path traversal validation.	2026-08-10	5.5	CVE-2026-15059
TangibleWP--Vehica Core	Subscriber Server Side Request Forgery (SSRF) in Vehica Core <= 1.0.104 versions.	2026-08-13	6	CVE-2026-66654
Tenable, Inc.--Security Center	An issue was identified in which CSRF tokens were generated using a predictable method, potentially reducing their effectiveness as a security control. This has been addressed by improving the randomness and entropy of token generation.	2026-08-14	5.3	CVE-2026-19636
Tenable, Inc.--Security Center	A SQL injection vulnerability exists in Security Center that could allow an authenticated administrator to execute arbitrary SQL queries, potentially resulting in unauthorized access to sensitive data, including credentials.	2026-08-14	4.9	CVE-2026-19631

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Tenable, Inc.-- Security Center	An improper access control vulnerability exists where an authenticated non-administrative application user could potentially view settings outside of their assigned scope.	2026-08-14	4.3	CVE-2026-19639
The OpenNMS Group--Meridian	A JEXL expression sandbox bypass exists in multiple versions of OpenNMS Meridian and Horizon. A low-privileged authenticated user can submit a crafted expression to the Measurements REST API that escapes the sandbox and loads arbitrary Java classes on the server. This can potentially allow an attacker to gain access to confidential information and compromise integrity. The solution is to upgrade to Meridian 2024.3.12, 2025.0.9 and Horizon 36.0.3 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	2026-08-13	5.4	CVE-2026-19135
The OpenNMS Group--Meridian	An incorrect authorization check in the v2 Alarm REST API in OpenNMS Meridian and Horizon allows a low-privileged authenticated user (ROLE_REST) to acknowledge, escalate, or clear alarms recorded as an arbitrary username, and, when also assigned ROLE_READONLY, to modify alarm state despite the read-only restriction. A credential check that should restrict these operations is guarded by an inverted condition, so it never executes for a real (non-blank) username. This can potentially allow an attacker to compromise the integrity of alarm state and audit records. The solution is to upgrade to Meridian 2024.3.12, 2025.0.9 and Horizon 36.0.3 or newer. Meridian and Horizon installation instructions state that they are intended for installation within an organization's private networks and should not be directly accessible from the Internet.	2026-08-13	4.3	CVE-2026-19182
themefic--Hydra Booking Appointment Scheduling & Booking Calendar	The Hydra Booking - Appointment Scheduling & Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'first_name' parameter in all versions up to, and including, 1.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with host-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The tfhb_host role required to exploit this vulnerability can be self-assigned by any visitor via the plugin's public Signup shortcode, making this effectively exploitable by unauthenticated users who complete the registration flow.	2026-08-15	6.4	CVE-2026-15948
themefic--Tourfic	Subscriber Broken Access Control in Tourfic <= 2.23.1 versions.	2026-08-13	6.5	CVE-2026-27999
Themepoints--Accordion	Subscriber Cross Site Scripting (XSS) in Accordion <= 3.0.6 versions.	2026-08-13	6.5	CVE-2026-66471
themeum--Kirki Freeform Page Builder, Website Builder & Customizer	The Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the post_meta Shortcode in all versions up to, and including, 6.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-11	6.4	CVE-2026-16974
themeum--Kirki Freeform Page Builder, Website Builder & Customizer	The Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 6.1.1 via the 'data' parameter parameter. This makes it possible for authenticated attackers, with editor-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. The intended strpos()-based guard against leaving the uploads directory is bypassed by crafting a URL that includes the uploads base path as a substring while embedding directory traversal sequences, such as /wp-content/uploads/../../wp-config.php.	2026-08-16	4.9	CVE-2026-17604
themeum--Kirki Freeform Page Builder, Website	The Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.1.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with custom-	2026-08-16	4.3	CVE-2026-18347

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Builder & Customizer	level access and above, to read arbitrary user metadata and sensitive user record fields - including email address, assigned roles, registration date, and any user_meta values - belonging to any WordPress user including administrators, by supplying a target user ID with a user-type context to the frontend collection endpoint.			
timwhitlock--Loco Translate	The Loco Translate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via PO File Extracted Comments in all versions up to, and including, 2.8.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with translator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-16	6.4	CVE-2026-15066
Toast Plugins--Internal Link Optimiser	Unauthenticated Broken Access Control in Internal Link Optimiser <= 5.2.7 versions.	2026-08-13	6.5	CVE-2026-66464
toocheke--Toocheke Companion	The Toocheke Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including, 2.10 via the 'series_bg_color' post meta field. This is due to insufficient input sanitization in the toocheke_series_bg_color_save() function (which stores the raw \$_POST value in post meta) and insufficient output escaping in the series admin column rendering (where the stored value is concatenated into a style attribute without esc_attr()). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user, such as an administrator, accesses the series list table in the admin dashboard.	2026-08-16	6.4	CVE-2026-15604
ToolJet--ToolJet	ToolJet is the open-source foundation am AI-native platform for building and deploying internal tools, workflows and AI agents. Prior to 3.20.207, the ToolJet Database HTTP API in server/src/modules/tooljet-db/controller.ts authorizes operations against the :organizationId URL path value without verifying that the caller belongs to that organization. JwtAuthGuard validates the tj-workspace-id header against the caller's memberships, while server/src/modules/tooljet-db/ability/index.ts grants VIEW_TABLES, VIEW_TABLE, and JOIN_TABLES without binding them to the path organization. An authenticated user can set tj-workspace-id to the user's own workspace and target another workspace through GET /api/tooljet-db/organizations/:organizationId/tables, GET /api/tooljet-db/organizations/:organizationId/table/:tableName, POST /api/tooljet-db/organizations/:organizationId/join, and the related table-management routes, allowing disclosure of table names, schemas, and rows and allowing tables to be created, altered, bulk populated, or dropped across tenant boundaries. This issue is fixed in version 3.20.207-lts.	2026-08-11	5.9	CVE-2026-73068
trainingbusinesspros--Groundhogg CRM, Newsletters, and Marketing Automation	The Groundhogg - CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to generic SQL Injection via the 'tag_query' parameter in all versions up to, and including, 4.5.14 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with vendor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the attacker to trigger the vulnerable Legacy_Contact_Query code path by submitting an unknown filter type (e.g. filters[0][0][type]=force_fallback), which causes a FilterException that dispatches execution away from the modern query handler.	2026-08-15	6.5	CVE-2026-18387
TRENDnet--TEW-816DRM	A vulnerability was found in TRENDnet TEW-816DRM GURNC4.OT182B-C-TN-R1B028-US.EN. This impacts an unknown function of the file /etc/bftpd.conf of the component bftpd. The manipulation of the argument USERLIMIT_GLOBAL results in allocation of resources. It is possible to launch the attack remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2026-08-14	5.3	CVE-2026-19830

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
triggerdotdev--trigger.dev	Trigger.dev is a platform for building and deploying fully managed AI agents and workflows. From 4.4.2 until 4.5.0-rc.4, `POST /api/v1/runs/:runParam/replay` in apps/webapp/app/routes/api.v1.runs.\$runParam.replay.ts uses `prisma.taskRun.findUnique({ where: { friendlyId: runParam } })` without a runtimeEnvironmentId filter, then ReplayTaskRunService in apps/webapp/app/v3/services/replayTaskRun.server.ts replays the selected run in the victim environment. Any valid environment API key can therefore replay another tenant's run by friendlyId, consuming victim resources and repeating side effects; when `payloadType: "application/store"` is used, overrideExistingPayloadPacket() calls conditionallyImportPacket() on existingTaskRun.payload without an integrity check, so payload bytes overwritten through a separate object-store path-traversal vulnerability become attacker-controlled input to the victim task. This issue is fixed in version 4.5.0-rc.4.	2026-08-13	4.2	CVE-2026-73657
tursodatabase--turso-cli	Turso CLI is the command line interface (CLI) to the open-source database Turso. Versions prior to 1.0.26 persist the user's Turso platform JWT to `settings.json` using Viper's default `configPermissions` of `0o644`, leaving the credential file world-readable on standard Linux and macOS systems. Any other local UID on the host can read the file and recover the platform JWT, which grants full Turso platform access scoped to the user's organizations. Version 1.0.26 patches the issue.	2026-08-11	5.5	CVE-2026-48790
Typemill--Typemill	Typemill CMS version 2.x contains a persistent cross-site scripting vulnerability in the Markdown parser extension that allows authenticated users with theme-configuration access to inject malicious JavaScript URLs by supplying unsanitized href values in Markdown links. Attackers can craft Markdown links using the javascript: scheme through ParsedownExtension.php or TwigMarkdownExtension.php, storing a persistent payload that executes in the browser of every visitor who clicks the link, enabling session cookie theft, authenticated request forgery, and credential harvesting.	2026-08-10	4.8	CVE-2026-44401
typeorm--typeorm	TypeORM is a TypeScript and JavaScript ORM for Node.js that supports PostgreSQL, MySQL, MariaDB, SQLite, SQL Server, Oracle, and other databases. Prior to versions 0.3.31 and 1.1.0, typeorm migration:generate embeds database schema metadata into JavaScript or TypeScript template literals in src/commands/MigrationGenerateCommand.ts, escaping backticks but not \${...} interpolation. An attacker with database schema write access can place a payload in column COMMENT or DEFAULT metadata, or another introspected schema string, and the JavaScript engine evaluates the payload when the generated migration is loaded through migration:run, import, or require. This issue is fixed in versions 0.3.31 and 1.1.0.	2026-08-13	5.7	CVE-2026-73651
Ultimate Fosters--Ultimate POS (Stock Management & Point of Sale)	Ultimate POS (Stock Management & Point of Sale) contains a stored cross-site scripting vulnerability that allows low-privileged authenticated attackers to inject arbitrary HTML and script markup by setting a malicious payload in the user first-name field during account creation. Attackers with a low-privileged role such as Cashier can submit a leave request through the HRM/Leave module, causing the unsanitized first-name markup to execute in the browser session of any higher-privileged user who views the leave-application notification pane, enabling cross-user session compromise within the admin origin.	2026-08-12	5.4	CVE-2026-70560
Universal Software Inc.--E-Municipality	Authentication bypass by primary weakness vulnerability in Universal Software Inc. E-Municipality allows Exploitation of Trusted Identifiers. This issue affects E-Municipality: from 20251127 before 20260204.	2026-08-14	5.3	CVE-2026-1621
usmannasir--cyberpanel	CyberPanel 2.4.3, fixed in commit eca0c3c, contains an arbitrary file read vulnerability in the file manager component that allows authenticated attackers to read sensitive system files by uploading a crafted ZIP archive containing symbolic links. Attackers can exploit the application's failure to validate symlinks before extraction, causing symbolic links targeting arbitrary filesystem paths outside the	2026-08-10	6.5	CVE-2026-71964

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user's home directory to persist on disk and be accessed through the web interface.			
usmannasir--cyberpanel	CyberPanel before 3.0.0 contains a path traversal vulnerability that allows authenticated administrators to read arbitrary files from the server filesystem by supplying unsanitized file paths to the cloudAPI ReadReport endpoint. Attackers can manipulate the reportFile parameter in the JSON request body, which is passed directly to open() in cloudManager.py without validation or allowlisting, enabling traversal to any file readable by the root-privileged CyberPanel process including credential files, SSL and SSH private keys, and JWT secret files.	2026-08-13	4.9	CVE-2026-67613
vllm-project--vllm	vLLM is an inference and serving engine for large language models. From 0.19.0 until 0.26.0, the /v1/completions CompletionRequest.prompt field in vllm/entrypoints/openai/completion/protocol.py accepts an unbounded list[str] or list[list[int]], prompt_to_seq() in vllm/renderers/inputs/preprocess.py and OnlineRenderer.preprocess_completion() in vllm/renderers/online_renderer.py expand every element, and vllm/entrypoints/openai/completion/serving.py creates one engine generator and response slot per prompt, allowing an authenticated API client to exhaust CPU, memory, async scheduling capacity, engine request slots, and response buffering with one request. This issue is fixed in version 0.26.0.	2026-08-13	6.5	CVE-2026-73559
vllm-project--vllm	vLLM is an inference and serving engine for large language models. Prior to 0.26.0, the validation_exception_handler in vllm/entrypoints/openai/server_utils.py converts FastAPI RequestValidationError objects with str(exc), and sanitize_message in vllm/entrypoints/utils.py does not remove traceback-style file paths, allowing unauthenticated malformed JSON requests to /v1/chat/completions, /v1/completions, /tokenize, and /detokenize to disclose the OS username, home and virtual-environment paths, Python version, internal package structure, line numbers, and endpoint handler names. This issue is fixed in version 0.26.0.	2026-08-13	5.3	CVE-2026-73555
vllm-project--vllm	vLLM is an inference and serving engine for large language models. Prior to 0.26.0, the structured_outputs.regex parameter in vllm/v1/structured_output/backend_lm_format_enforcer.py is passed to lmformatenforcer.RegexParser without compile_regex_with_timeout or validation in validate_structured_output_request_lm_format_enforcer, allowing an unauthenticated /v1/completions request against the lm-format-enforcer backend to consume a CPU core and stall the structured-output engine path with a catastrophic regular expression. This issue is fixed in version 0.26.0.	2026-08-13	5.3	CVE-2026-73556
vllm-project--vllm	vLLM is an inference and serving engine for large language models. Prior to 0.27.0, an integer overflow in blockIdx.x * 2 * d in activation_kernels.cu can cause act_and_mul_kernel to consume another batched user's input, allowing a request processed in the same inference batch to receive a partial or complete copy of another user's inference result. This issue is fixed in version 0.27.0.	2026-08-13	5.3	CVE-2026-73558
vmoranv--jshookmcp	@jshookmcp/jshook is an MCP server that gives AI agents tools for JavaScript analysis and security research. In version 0.3.1, the network domain has a central SSRF authorization policy that blocks private, loopback, link-local, and reserved targets unless an explicit authorization object allows private network access. The policy is enforced by raw HTTP/TCP/TLS RTT tools, but the ICMP probe and traceroute tools resolve the target and invoke the native ICMP/traceroute sink directly. An MCP client with access to an active network domain can therefore ask the jshookmcp server to probe internal addresses even when local SSRF access is disabled for the other raw network tools. This exposes an internal reachability and route mapping primitive from the server network position. Version 0.3.2 fixes the issue.	2026-08-13	4.3	CVE-2026-49856
Wallet System for WooCommerce--	The Wallet System for WooCommerce WordPress plugin before 2.7.10 does not validate a user-supplied wallet amount against the customer's actual stored	2026-08-12	6.5	CVE-2026-15045

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Wallet System for WooCommerce	balance during checkout, allowing authenticated customers to arbitrarily reduce their own order total, including down to zero, and complete checkout without paying the merchant.			
wcproducttable--Product Table & List Builder For WooCommerce	The WC Product Table Lite plugin for WordPress is vulnerable to CSS Injection in versions up to, and including, 5.6.0 via the 'laptop_scroll_offset' shortcode attribute exposed through the unauthenticated wcpt_ajax() AJAX handler. The handler is registered for wp_ajax_nopriv_wcpt_ajax, JSON-decodes attacker-supplied attributes, only allowlists key names (not values), applies a preg_replace that strips only [] < >, and passes the value through do_shortcode into wcpt_style__sticky_sidebar(), where it is interpolated verbatim into inline CSS ('top: {\$top}px;' and 'max-height: calc(100vh - {\$top}px);') with no numeric casting or CSS escaping. This makes it possible for unauthenticated attackers to inject arbitrary CSS declarations and rules on pages rendering a product table with sticky sidebar enabled, which can be leveraged for data exfiltration (via attribute-selector + background-image URLs), UI redressing, and phishing that bypasses CSPs permitting inline styles.	2026-08-16	5.3	CVE-2026-15441
wcvendors--WC Vendors WooCommerce Multivendor, WooCommerce Marketplace, Product Vendors	The WC Vendors - WooCommerce Multivendor, WooCommerce Marketplace, Product Vendors plugin for WordPress is vulnerable to generic SQL Injection via the 'status' parameter in all versions up to, and including, 2.7.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with shop manager-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The sanitize_text_field callback strips HTML but leaves SQL metacharacters intact, and wp_magic_quotes slash protection does not apply because WP_REST_Server::serve_request() calls wp_unslash() on GET parameters before the sanitize callback executes.	2026-08-16	4.9	CVE-2026-15351
webaways--NEX-Forms Ultimate Forms Plugin for WordPress	The NEX-Forms - Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to generic SQL Injection via the 'additional_params' parameter in all versions up to, and including, 9.2.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with admin-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is a second-order vulnerability; the payload is stored via the submission_report2 AJAX handler (which lacks a nonce check and relies solely on a capability that can be configured down to subscriber-level) and triggered when a CSV export is generated.	2026-08-16	4.9	CVE-2026-15602
webhosting4ugr--Secure Card Gateway for ePay Paycenter (Piraeus Bank)	Unauthenticated Broken Access Control in Secure Card Gateway for ePay Paycenter (Piraeus Bank) <= 1.0.32 versions.	2026-08-13	6.5	CVE-2026-61978
Webkul--Bagisto	A vulnerability was determined in Webkul Bagisto up to 2.4.4. Affected is an unknown function of the file /admin/customers/login-as-customer/ of the component Admin Customer Impersonation Feature. This manipulation of the argument ID causes authorization bypass. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."	2026-08-14	4.7	CVE-2026-19834
Webkul--Bagisto	A security flaw has been discovered in Webkul Bagisto up to 2.4.4. Affected by this issue is some unknown functionality of the file /admin/customers/view of the component Backend Customer Detail Feature. Performing a manipulation of the	2026-08-14	4.3	CVE-2026-19836

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	argument ID results in authorization bypass. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."			
Webkul--Bagisto	A security vulnerability has been detected in Webkul Bagisto up to 2.4.4. This vulnerability affects unknown code of the file /admin/reporting/sales/ of the component Backend Reporting Endpoint. The manipulation leads to authorization bypass. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."	2026-08-14	4.3	CVE-2026-19838
weblizar--Admin Custom Login	The Admin Custom Login plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.6.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2026-08-16	4.4	CVE-2026-2487
weblizar--The School Management Education & Learning ERP	The The School Management - Education & Learning ERP plugin for WordPress is vulnerable to generic SQL Injection via 'order[0][dir]' Parameter in all versions up to, and including, 5.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This vulnerability is replicated across seven or more AJAX handlers including wlsn-fetch-staff-classes, wlsn-fetch-notices, wlsn-fetch-subjects, wlsn-fetch-inquiries, wlsn-fetch-staff-employee, and wlsn-fetch-payments, and the missing nonce verification on several of these handlers also enables CSRF-chained exploitation.	2026-08-16	6.5	CVE-2026-9767
Welcart e-Commerce--Welcart e-Commerce	The Welcart e-Commerce WordPress plugin before 2.11.33 does not verify the authenticity of its convenience-store / bank-transfer settlement callback: an unauthenticated request can flip an order from unpaid to settled purely from an order number and a status flag, with no signature, amount, or origin check. Because these are pay-later methods, an attacker can mark their own unpaid order as settled and obtain fulfilment without paying.	2026-08-12	5.3	CVE-2026-15213
Windmill Labs--Windmill	An information disclosure vulnerability in Windmill Labs Windmill through 1.783.0 allows any authenticated workspace member to read legacy ownerless draft scripts that contain plaintext resource credentials. Drafts with a null owner email bypass ACL enforcement and are returned to any workspace member who queries the drafts endpoint. Sensitive credentials stored in these drafts are exposed across ACL boundaries.	2026-08-11	6.5	CVE-2026-72539
Windmill Labs--Windmill	A missing authorization vulnerability in Windmill Labs Windmill through 1.783.0 allows any authenticated workspace member to overwrite any resource type schema via the update_resource_type endpoint. The endpoint omits the administrator permission check that the corresponding delete_resource_type endpoint enforces. An attacker with workspace member privileges can corrupt resource type definitions, breaking workflows that depend on them.	2026-08-11	6.5	CVE-2026-72541

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Windmill Labs--Windmill	A missing authorization vulnerability in Windmill Labs Windmill through 1.783.0 allows authenticated operators to write job progress and read job metrics for any job in the workspace regardless of ownership. The job_metrics handlers accept no authorization extractor, bypassing workspace-level access controls. An operator can monitor sensitive job execution data and inject misleading progress for jobs they do not own.	2026-08-11	5.4	CVE-2026-72542
Wireshark Foundation--Wireshark	Ixia IxVeriWave and Vector Informatik BLF file parser crashes in 4.6.0 to 4.6.7 allows denial of service on Windows	2026-08-13	6.6	CVE-2026-19696
Wireshark Foundation--Wireshark	TTX Logger file parser crash in 4.6.0 to 4.6.7 allows denial of service	2026-08-13	4.7	CVE-2026-19694
Wireshark Foundation--Wireshark	Gammu DCT3 trace file parser crash in 4.6.0 to 4.6.7 allows denial of service	2026-08-13	4.7	CVE-2026-19695
WP Umbrella--WP Umbrella	Cross-Site Request Forgery (CSRF) vulnerability in WP Umbrella allows Cross Site Request Forgery. This issue affects WP Umbrella: from 2.24.2 through 2.26.2.	2026-08-10	5.4	CVE-2026-66642
wpdevart--Booking calendar, Appointment Booking System	The Booking calendar, Appointment Booking System plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.2.36. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to mark arbitrary reservations as paid or completed, cancel legitimate payments, auto-approve reservations, and trigger transactional booking emails by writing attacker-supplied payment status and transaction data directly into the payments table. The auto-approval of reservations is only triggered when the 'enable_psuccess_approval' site option is enabled, but payment status manipulation and email dispatch are exploitable regardless of that setting.	2026-08-15	5.3	CVE-2026-8840
wpeverest--Everest Forms Contact Form, Payment Form, Quiz, Survey & Custom Form Builder with AI	The Everest Forms - Contact Form, Payment Form, Quiz, Survey & Custom Form Builder with AI plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.5.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with delegated form management access and above, to activate arbitrary already-installed WordPress plugins - including previously deactivated or vulnerable plugins - without holding the core activate_plugins capability. Exploitation requires the target user to hold a delegated Everest Forms capability (manage_everest_forms, everest_forms_create_forms, or everest_forms_view_forms), which the plugin's own roles and permissions tool allows administrators to assign to non-administrator roles such as Author; the nonces required to exploit the AJAX handlers are emitted on EVF admin pages accessible to any such delegated user.	2026-08-16	4.3	CVE-2026-13167
wpeverest--User Registration	Unauthenticated Broken Access Control in User Registration <= 5.2.6 versions.	2026-08-13	5.3	CVE-2026-73403
WPManageNinja--FluentCommunity	Subscriber Cross Site Scripting (XSS) in FluentCommunity <= 2.7.5 versions.	2026-08-13	6.5	CVE-2026-66467
WPML--WPML Multilingual CMS	The WPML Multilingual CMS plugin for WordPress is vulnerable to SQL Injection via the 'sorting' parameter in all versions up to, and including, 4.9.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with translator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-15	6.5	CVE-2026-12248

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpmonks--Gravity Booster Styles & Layouts for Gravity Forms	The Gravity Booster - Styles & Layouts for Gravity Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 5.26 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where <code>unfiltered_html</code> has been disabled.	2026-08-16	4.4	CVE-2026-12477
wpmudev--Forminator Forms Contact Form, Payment Form & Custom Form Builder	The Forminator Forms - Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.55.0.2 via the 'draft' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to enumerate sequential integer entry IDs via the 'draft' parameter and read other users' saved draft form data, including names, email addresses, phone numbers, addresses, and free-form message content. This is only exploitable on forms that have the 'Save and Continue' feature enabled.	2026-08-16	5.3	CVE-2026-12998
wpweaver--Turnkey bbPress by WeaverTheme	The Turnkey bbPress by WeaverTheme plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.7.1 via deserialization of untrusted input in the <code>wvrbbp_set_to_serialized_values()</code> function (reached through the <code>wvrbbp_save_restore()</code> settings-restore handler). The function reads the raw contents of an administrator-uploaded file and passes them directly to <code>unserialize()</code> without any validation. This makes it possible for authenticated attackers, with administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin itself; however, if a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	2026-08-16	6.6	CVE-2026-10035
xpf0000--FlyEnv	FlyEnv before 4.18.0 fails to sanitize HTML from markdown rendering and AI chat content passed to Vue v-html directives. Attackers can inject malicious scripts through markdown sources or chat messages that execute in the Electron renderer process with access to Node.js APIs and the filesystem.	2026-08-10	6.1	CVE-2026-69116
zephyrproject--zephyr	The Intel ALH digital-audio-interface driver function <code>dai_alh_get_properties()</code> in <code>drivers/dai/intel/alh/alh.c</code> used a caller-supplied <code>int stream_id</code> with no range validation. The value indexes the fixed-size static <code>const uint8_t alh_handshake_map[64]</code> array and scales a FIFO register address, so an out-of-range <code>stream_id</code> produces an out-of-bounds read of one byte at an attacker-chosen signed offset from the array. That byte is written into <code>prop->dma_hs_id</code> and the resulting struct <code>dai_properties</code> is copied back to the caller, leaking it. <code>dai_get_properties_copy()</code> is a Zephyr <code>__syscall</code> , and its verifier <code>z_vrfy_dai_get_properties_copy()</code> (<code>drivers/dai/dai_handlers.c</code>) validates only the device-object permission and the destination buffer, not <code>stream_id</code> . A user-mode thread that has been granted access to the ALH DAI device object can therefore call the syscall with an arbitrary <code>stream_id</code> , crossing the userspace/kernel sandbox boundary. The impact is a one-byte-per-call arbitrary-offset kernel information disclosure (and leakage of a computed kernel address via <code>fifo_address</code>); a <code>stream_id</code> that resolves to an unmapped page faults in kernel context, giving a local denial of service. Exploitation requires <code>CONFIG_USERSPACE</code> and device access, making this a local, moderate-severity issue. The fix rejects negative and too-large <code>stream_id</code> values up front and returns <code>NULL</code> , which the copy wrapper maps to <code>-ENOENT</code> .	2026-08-12	6.1	CVE-2026-12232
zephyrproject--zephyr	The Linkable Loadable Extensions (llex) subsystem mis-handles PLT/RELA relocation entries when linking a relocatable (partially-linked) ELF extension. In <code>llex_link_plt()</code> (<code>subsys/llex/llex_link.c</code>), the relocatable branch (<code>tgt != NULL</code> , the path used for Xtensa relocatable objects) computed the patch address as <code>ext->mem[LLEX_MEM_TEXT] - text.sh_offset + rela.r_offset + tgt->sh_offset</code> and then performed the relocation write there without validating <code>rela.r_offset</code> . Its sibling <code>shared/dynamic</code> branch already rejected out-of-range offsets via <code>llex_file_offset()</code> . <code>rela.r_offset</code> is read directly from the ELF's RELA table, so a crafted entry with an	2026-08-12	6.3	CVE-2026-12235

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	offset larger than the target section makes the write land arbitrarily far outside the extension's text buffer. The result is an attacker-influenced out-of-bounds write (the location via <code>r_offset</code> , the written value being the resolved symbol address) performed in supervisor context at link time, before any extension code runs. The path is reached from <code>llex_load()</code> whenever an application loads an attacker-influenced ELF extension on Xtensa with writable storage; <code>llex</code> is documented to accept extensions of untrusted origin. Impact is supervisor-context memory corruption (integrity and availability loss, and a sandbox-boundary escape for user-mode extensions). Exploitation is gated by the Xtensa relocatable PLT path and writable storage, and turning the out-of-range write into a useful primitive is non-trivial. The fix adds a bound check rejecting any RELA entry whose <code>r_offset >= tgt->sh_size</code> , mirroring the existing validation in the shared branch.			
zephyrproject--zephyr	The Bluetooth host GATT client function <code>parse_read_std_char_desc()</code> in <code>subsys/bluetooth/host/gatt.c</code> parses an ATT Read By Type Response received from a remote GATT server during <code>BT_GATT_DISCOVER_STD_CHAR_DESC</code> discovery. The per-entry stride <code>rsp->len</code> is taken directly from the peer's PDU, and the parse loop both tests its exit condition (<code>length >= rsp->len</code>) and advances (<code>length -= rsp->len</code> , <code>pdu += rsp->len</code>) using that value. The minimum value of <code>rsp->len</code> was never validated before the loop. A malicious or malfunctioning peer can reply with <code>rsp->len = 0</code> . Because <code>length</code> is unsigned and never decreases, the loop condition stays true forever and the read pointer never advances; as long as the body is at least a few bytes with a non-zero handle and a matching descriptor UUID, the host repeatedly re-parses the same bytes and invokes the discovery callback, never terminating. This hangs the Bluetooth host processing thread (CWE-835, loop with unreachable exit condition). The condition is reachable by any connected peer once the local device initiates standard-descriptor-value discovery; GATT discovery does not require bonding or encryption, so an unauthenticated adjacent attacker that the device connects to can trigger it. The impact is denial of service of the Bluetooth subsystem (and likely a watchdog reset on constrained targets); there is no memory disclosure or corruption. The fix adds a <code>rsp->len < sizeof(struct bt_att_data)</code> check before the loop, rejecting under-length responses so the stride is always non-zero and the loop terminates. The sibling parsers <code>parse_include()</code> and <code>parse_characteristic()</code> already validated <code>rsp->len</code> and are unaffected.	2026-08-13	6.5	CVE-2026-12236
zephyrproject--zephyr	The Bluetooth HCI driver for Bouffalo Lab on-chip BLE controllers (BL60x/BL70x/BL61x), <code>bt_bflb_send()</code> in <code>drivers/bluetooth/hci/hci_bflb.c</code> , violates the <code>bt_hci_driver_api.send()</code> buffer-ownership contract. That contract (documented at <code>include/zephyr/drivers/bluetooth.h</code>) requires the buffer reference to be consumed only on success; on error the caller still owns the reference and unrefs it. The driver instead routed all error paths through a shared label that unconditionally called <code>net_buf_unref(buf)</code> before returning the error code, consuming the buffer on failure as well. When <code>send()</code> returns an error, the host TX path (<code>send_buf()</code> in <code>subsys/bluetooth/host/conn.c</code>) unrefs the same buffer again, believing it still owns it. This double-unref over-decrements the <code>net_buf</code> reference count. Because the buffer is a TX fragment whose destroy callback also decrements its still-queued parent buffer, the parent is freed prematurely while reachable on the connection TX queue, producing a use-after-free and corruption of the shared <code>net_buf</code> pool rather than a benign leak. The error conditions are on the host-to-controller transmit path (controller send failure, or an unsupported H:4 packet type), so they are not driven directly by attacker-supplied radio bytes; a remote/adjacent peer can influence them only indirectly, e.g. by inducing controller TX failures under heavy link load. The consequence when reached is BLE-stack denial of service (crash / pool corruption) with possible further memory corruption, bounded to devices using one of these Bouffalo Lab on-chip controllers.	2026-08-11	5.9	CVE-2026-11893
zephyrproject--zephyr	The Realtek BEE Bluetooth HCI driver's send callback, <code>bt_hci_bee_send()</code> in <code>drivers/bluetooth/hci/hci_bee.c</code> , violated the <code>bt_hci_driver_api</code> buffer-ownership contract. That contract requires the driver to consume (unref) the transmit <code>net_buf</code>	2026-08-11	5.9	CVE-2026-11894

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	only on success; on an error return the host caller retains ownership and unrefs the buffer itself. The pre-fix code routed all error paths through a shared cleanup label that unconditionally called <code>net_buf_unref(buf)</code> before returning the error code. Because the host TX paths (in <code>subsys/bluetooth/host/hci_core.c</code>) unref the buffer again after <code>send()</code> returns an error, the buffer is freed twice: the driver returns it to its <code>net_buf</code> pool and the host then unrefs the already-freed buffer, corrupting the shared pool / underflowing the reference count (CWE-415). The same error branch additionally dereferenced <code>buf->len</code> inside a <code>LOG_ERR</code> call after the buffer had already been unref'd, a read of freed memory (CWE-416) that is compiled in at the default error log level. The failing edges are reached when the controller's host-to-controller buffer allocation fails or the controller send fails (resource-exhaustion / IO conditions). A remote Bluetooth peer can push the device toward these conditions indirectly by driving heavy host transmit activity, at which point the double-free corrupts the host <code>net_buf</code> pool and most likely crashes the device, with residual potential for further memory corruption. The impact is confined to builds using this specific Realtek BEE HCI driver. The fix returns early from each error path without unrefing and unrefs the buffer only on the success path, restoring the ownership contract and eliminating both the double-free and the use-after-free read.			
zephyrproject--zephyr	The USB device-side CDC NCM class control-to-host handler <code>usbd_cdc_ncm_cth</code> in <code>subsys/usb/device_next/class/usbd_cdc_ncm.c</code> builds a fixed-size response for the <code>GET_NTB_PARAMETERS</code> (28-byte struct <code>ntb_parameters</code>) and <code>GET_NTB_INPUT_SIZE</code> (8-byte struct <code>ntb_input_size</code>) class requests and copies the whole structure into the control DATA IN buffer with <code>net_buf_add_mem(buf, ..., sizeof(...))</code> , ignoring the host-supplied <code>wLength</code> . The control DATA IN buffer is allocated by the USB stack with a capacity of exactly <code>wLength</code> bytes (<code>usbd_ep_ctrl_data_in_alloc -> udc_ctrl_data_alloc -> net_buf_alloc_len(&udc_ep_pool, wLength)</code> ; no round-up is applied for the IN endpoint). Because <code>net_buf_add_mem/net_buf_simple_add</code> only bounds the copy with an <code>__ASSERT_NO_MSG</code> , which is compiled out in production builds, a host that issues one of these standard CDC NCM control requests with a <code>wLength</code> smaller than the response structure (e.g. <code>wLength = 1</code>) causes the handler to <code>memcpy</code> up to 27 bytes past the end of the allocated pool buffer. The request fields come straight from the USB SETUP packet, so any host (or USB interposer) the Zephyr device enumerates against can trigger the overflow with no authentication once an image built with the <code>device_next</code> USB stack and the CDC NCM class is connected. The out-of-bounds write corrupts adjacent allocations and metadata in the shared <code>udc_ep_pool</code> , primarily causing memory corruption and denial of service of the USB stack; the overflow length is bounded (<code><= 27</code> bytes) and the written content is fixed device constants, and the bug reads nothing back so there is no information disclosure. The fix clamps the copy with <code>MIN(sizeof(...), setup->wLength)</code> , matching the existing CDC ACM handler.	2026-08-11	5.2	CVE-2026-12052
zephyrproject--zephyr	The PSA Protected Storage credential backend (<code>subsys/net/lib/tls_credentials/tls_credentials_trusted.c</code>) declared its credential-store mutex as a plain zero-filled static struct <code>k_mutex credential_lock</code> ; and never called <code>k_mutex_init()</code> on it. A statically zero-filled <code>k_mutex</code> has an uninitialized wait queue (its <code>dlist</code> head/tail are <code>NULL</code> instead of the self-referential sentinels that <code>k_mutex_init/K_MUTEX_DEFINE</code> install). The uncontended lock path does not touch the wait queue, so the defect is latent and serialized use behaves correctly. When two execution contexts contend on the lock, <code>k_mutex_lock()</code> pends the blocking thread on the wait queue via <code>z_pend_curr()</code> , which calls <code>sys_dlist_append()</code> on the zeroed list and dereferences a <code>NULL</code> tail pointer (<code>tail->next = node</code>), faulting the kernel. The lock is held during TLS handshake credential loading and by all credential add/get/delete operations, so a deployment performing concurrent TLS handshakes (for example a server handling multiple simultaneous connections from a remote peer) or a credential-management operation concurrent with a handshake can trigger the dereference. The impact is a denial of service: a deterministic kernel panic / device reset on the first	2026-08-12	5.9	CVE-2026-12233

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contention. There is no memory corruption beyond the NULL dereference and no confidentiality or integrity impact; mutual exclusion on the fast path remains correct. Exposure is limited to builds with CONFIG_TLS_CREDENTIALS_BACKEND_PROTECTED_STORAGE enabled (PSA Protected Storage / TF-M platforms); the default volatile RAM backend initializes its lock correctly and is unaffected. The fix initializes the mutex statically with K_MUTEX_DEFINE(credential_lock), providing a valid wait queue so the contended path no longer touches a NULL list.			
zephyrproject--zephyr	A use-after-free exists in the Zephyr second-generation work queue (kernel/work.c) in the handling of delayable work timeouts. When a delayable work item's timeout has been dequeued and its handler work_timeout() is in flight (blocked acquiring the work-queue spinlock), a concurrent cancellation does not wait for that handler to finish. In unschedule_locked() the pre-fix code called z_abort_timeout(), which for an already-announcing record returns -EINVAL without removing it; cancel_async_locked() then observes the work as idle, so even k_work_cancel_delayable_sync() and k_work_flush_delayable() return without blocking on the in-flight handler. Because those are the APIs the kernel header documents as the safe way to cancel before freeing a k_work_delayable, a caller that frees the object immediately after a successful sync cancel can race the still-pending handler. work_timeout() subsequently dereferences the freed record: it reads to->ticks via z_is_timeout_handler_canceled() and, if the freed slot has been reused so the bail check fails, performs a read-modify-write of wp->flags (K_WORK_DELAYED_BIT) and submits work against a stale dw->queue pointer - a use-after-free read and write. The k_work API is kernel-mode only (no __syscall entry point), so this is a kernel-internal concurrency defect rather than a userspace privilege escalation. Triggering it requires an SMP build and a subsystem that schedules and then frees (or reschedules) a delayable work item in the narrow window while its timeout is announcing; an attacker able to influence the timing of such teardown (for example via connection churn driving subsystem timers) has a plausible but probabilistic path. The impact is kernel memory corruption or crash (denial of service). The fix makes unschedule_locked() wait, by spinning on z_try_abort_timeout() returning -EAGAIN while releasing and re-acquiring the work spinlock, until any in-flight handler completes before returning, and switches work_timeout() to atomic K_WORK_DELAYED_BIT ownership. This closes both the free-then-handler use-after-free and the related reschedule early-fire race.	2026-08-14	5.8	CVE-2026-12365
zephyrproject--zephyr	The USB DFU class implementation in Zephyr's new (experimental) device_next USB device stack contains a NULL pointer dereference in handle_download() (subsys/usb/device_next/class/usbd_dfu.c). The handler computes MIN(setup->wLength, buf->len) and passes buf->data to the image write callback without checking that the buf net_buf pointer is non-NULL. The handler is reached over the USB control endpoint, driven by the USB host. For a DFU_DNLOAD (download) request with no Data OUT stage - notably the zero-length terminating download that the DFU protocol uses to end a firmware transfer - the USB core invokes the class handler with a NULL buffer. After the device has been advanced to the DFU_DNLOAD_IDLE state (by sending one valid download block and a GET_STATUS), a zero-length DFU_DNLOAD reaches handle_download() with buf == NULL, dereferencing it. The result is a NULL+offset read that triggers a fatal CPU fault, i.e. a denial of service (device crash/reset). The attacker is whatever controls the USB host the device is attached to; DFU download support must be enabled with a registered image. There is no memory corruption or information disclosure - impact is limited to availability. The fix adds an explicit if (buf != NULL) guard so the callback receives a zero-length, NULL-data transfer instead of crashing.	2026-08-11	4.6	CVE-2026-12051
zephyrproject--zephyr	The LoRaWAN Fragmented Data Block Transport service (subsys/lorawan/services/frag_transport.c) does not validate the fragment counter in a received DATA_FRAGMENT command before forwarding it to the configured decoder. In frag_transport_package_callback() the value frag_counter = hdr->frag_index_n & 0x3FFF is taken directly from the downlink payload and passed to	2026-08-14	4.2	CVE-2026-12363

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the decoder, which derives an array index and flash offset as frag_counter - 1. DataFragment fragments are 1-indexed, so a frag_counter of 0 underflows that arithmetic. With the default Semtech/LoRaMAC-node decoder, this reaches FragDecoder.FragNbMissingIndex[fragCounter - 1] = 0; in FragDecoderProcess(), where fragCounter - 1 evaluates to -1 and writes a uint16_t zero out of bounds, just before the array and into the adjacent MatrixM2B recovery-matrix state of the static decoder object (CWE-787). A companion write derives a wild flash offset, but that path is rejected by the flash_area_write() bounds check. The in-tree low-memory decoder (frag_dec()) is not corrupted: its out-of-range bit-array and flash accesses are caught by sys_bitarray_ and flash_area_ bounds checks. The handler is the registered downlink callback for the fragmentation transport port, reachable whenever an active fragmentation session exists, so the triggering byte is attacker-influenceable LoRaWAN/FUOTA network input. Triggering it requires authenticated downlinks (LoRaWAN MAC session keys or a malicious/compromised network or FUOTA server) and an active fragmentation session. The impact is contained: corruption of decoder state and denial of the firmware-update (FUOTA) session rather than controllable memory corruption or code execution. The fix adds a transport-layer check that rejects frag_counter == 0, closing the defect for both decoder backends.			
Zimbra-- Collaboration	In Zimbra Collaboration (ZCS) before 10.1.17, a stored cross-site scripting (XSS) vulnerability exists in the Zimbra Classic Web Client due to insufficient sanitization of specific attachment content during inline preview. An attacker can send a crafted email containing a malicious attachment that, when previewed by a user, executes arbitrary JavaScript within the victim's browser session. Successful exploitation may allow an attacker to perform unauthorized actions on behalf of the victim user, potentially leading to data exfiltration or unauthorized access to sensitive information.	2026-08-13	6.1	CVE-2026-73572
Zimbra-- Collaboration	In Zimbra Collaboration (ZCS) before 10.1.17, weak cryptographic key generation vulnerability exists in the OnlyOffice integration. The zimbraDocumentEditingJwtSecret is generated using an insecure random number generator, resulting in insufficient entropy. An attacker who obtains a JWT signed with the generated secret may be able to recover the JWT signing secret through offline brute-force, potentially enabling JWT forgery.	2026-08-13	6.3	CVE-2026-73576
Zoom Communications-- Zoom Clients	Missing bounds check in the annotator function of Zoom Clients allows buffer over-read, which may allow a meeting participant to conduct a denial of service on another participant via network access.	2026-08-11	6.5	CVE-2026-53414
Zyxel Networks-- WAH7601	Exposure of sensitive system information to an unauthorized control sphere vulnerability in Zyxel Networks WAH7601 allows Web Application Fingerprinting. This issue affects WAH7601: through 20072026.	2026-08-10	6.5	CVE-2026-6373
9001--copyparty	Copyparty is a portable file server. Prior to 1.20.17, copyparty volumes with the dk or dks directory-key flag combined with the fk or fka file-key flag can convert a valid file key into a directory key, granting read access to the containing folder. This vulnerability was only reachable if both types of keys (filekeys and dirkeys) were manually enabled in the volume flags simultaneously. This issue is fixed in version 1.20.17.	2026-08-18	4.3	CVE-2026-70657
93digital--Typing Effect	Contributor Cross Site Scripting (XSS) in Typing Effect <= 1.3.7 versions.	2026-08-18	6.5	CVE-2026-66644
@fastify/busboy-- @fastify/busboy	@fastify/busboy is a multipart form-data parser for Node.js. Its multipart part-header parser splits header lines only on the two-byte carriage-return line-feed sequence, so a lone carriage return or line feed embedded in a part header is not treated as a line break and is carried verbatim into the parsed Content-Disposition filename and field name handed to the application. An attacker who uploads a file whose filename or field name contains a bare carriage return or line feed can inject control characters into consumers that trust the parser to return clean values,	2026-08-21	5.8	CVE-2026-74866

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	enabling filesystem filename pollution, log forging, or header injection when the value is forwarded to a carriage-return-sensitive sink. All versions of @fastify/busboy up to and including 3.2.1 are affected. The issue is fixed in version 3.2.2, which rejects any header line that still contains a bare carriage return or line feed. Users should upgrade to 3.2.2, and consumers such as @fastify/multipart should bump their @fastify/busboy dependency to pull in the fix.			
Adblock for Youtube Extension--Adblock for Youtube Extension	A weakness has been identified in Adblock for Youtube Extension up to 7.2.1 on Chrome. The impacted element is the function updateDynamicRules of the file contentscript.js of the component Event Listener. This manipulation of the argument yt-anti-adblock-detected causes improper authorization. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-17	5.4	CVE-2026-19986
Alaev--SEO Tools Extension	A vulnerability was detected in Alaev SEO Tools Extension up to 1.0.10 on Chrome. This impacts the function addDiv of the file src/popup.html of the component Popup UI. Performing a manipulation results in basic cross site scripting. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-17	4.3	CVE-2026-19988
Alex--Featured Video Plus	Contributor Cross Site Scripting (XSS) in Featured Video Plus <= 2.3.3 versions.	2026-08-18	6.5	CVE-2026-66637
alexta69--MeTube	A vulnerability was determined in alexta69 MeTube up to 2026.06.10. The impacted element is an unknown function of the file /download/.metube/cookies.txt of the component Cookie File Handler. This manipulation causes files or directories accessible. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2026.06.20 is sufficient to resolve this issue. Patch name: ce897ee00903bf7ded406f0d7852d95dd4164add. You should upgrade the affected component.	2026-08-22	5.3	CVE-2026-78051
alexselegidis--plainpad	Plainpad through 1.1.1, fixed in commit d3823fc, contains a missing rate limiting vulnerability that allows unauthenticated attackers to send unbounded login requests to the POST /v1/sessions endpoint due to dead code in App\Http\Kernel.php that is never instantiated under the Laravel 11+ skeleton, leaving the API throttle configuration unattached to any route. Attackers can exploit this by sending unlimited credential attempts with no lockout or CAPTCHA enforcement, and additionally trigger CPU exhaustion by forcing repeated bcrypt comparisons on each request.	2026-08-18	5.3	CVE-2026-73529
amirsanni--Mini-Inventory-and-Sales-Management-System	A security flaw has been discovered in amirsanni Mini-Inventory-and-Sales-Management-System 0.1. Affected is the function Transaction::getAll of the file application/models/Transaction.php. Performing a manipulation of the argument orderBy/orderFormat results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-20	6.3	CVE-2026-76785
AngleSharp--AngleSharp	AngleSharp is a .NET library for parsing angle bracket based hyper-texts. Prior to 1.5.0, MathAnnotationXmlElement in AngleSharp/Mathml/Dom/Internal/MathAnnotationXmlElement.cs is not treated as an HTML integration point when its encoding attribute is text/html or application/xhtml+xml, causing Consume in AngleSharp/Html/Parser/HtmlDomBuilder.cs to route tokens through foreign-content parsing instead of HTML parsing. A sanitizer can therefore observe a different DOM from the browser that reparses the serialized output. An attacker can combine this namespace differential with markup-breaking characters in an attribute value so that an element hidden from the sanitizer becomes active script-	2026-08-18	6.9	CVE-2026-54570

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	capable HTML after browser reparsing, resulting in mutation cross-site scripting. This issue is fixed in version 1.5.0.			
apostrophecms--apostrophe	ApostropheCMS is an open-source Node.js content management system. Prior to 3.6.2, the import-export module in packages/import-export/lib/formats/gzip.js constructs an attachment source path from the attacker-controlled _id, name, and extension fields in aposAttachments.json without ensuring that the resolved path remains under the extracted attachments directory, allowing an authenticated contributor to import a crafted archive, read a host file with an allowed extension, and publish the copied file at an unauthenticated uploads URL. This issue is fixed in version 3.6.2.	2026-08-17	6.5	CVE-2026-63667
apostrophecms--apostrophe	ApostropheCMS is an open-source Node.js content management system. Prior to 4.32.0, the page module's move() operation fails to enforce the destination parent's _create permission because its oldParent archive condition disables the check for ordinary moves, allowing an authenticated editor or contributor to use _targetId and _position through the page REST update endpoint to move a controlled page into a restricted subtree and make nudgeNewPeers() updateMany re-rank protected sibling pages. This issue is fixed in version 4.32.0.	2026-08-17	6.5	CVE-2026-63669
apostrophecms--apostrophe	ApostropheCMS is an open-source Node.js content management system. Prior to 2.17.6, sanitizeHtml() can pass disallowed executable markup through packages/sanitize-html/index.js when textarea or xmp is included in allowedTags because a literal solidus after the raw-text end-tag name is treated as text by htmlparser2 and the ontext handler emits that content without escaping, while a browser parses the following img onerror markup as active HTML. This issue is fixed in version 2.17.6.	2026-08-17	6.1	CVE-2026-63670
apoyl--[Aotuman] Grab WeChat Articles	Subscriber Server Side Request Forgery (SSRF) in [Aotuman] Grab WeChat Articles <= 2.0.1 versions.	2026-08-18	6	CVE-2026-32467
appwrite--templates	The github-issue-bot templates in appwrite/templates verify the GitHub webhook signature with an inverted condition. verifyWebhook in node/github-issue-bot/src/github.js and in node/typescript/github-issue-bot/src/github.ts returns "typeof signature !== 'string' (await verify(...))", so when the X-Hub-Signature-256 header is absent the first operand is true, the logical OR short-circuits, and the function reports success without performing any HMAC verification. main.js rejects a request only when verifyWebhook returns false, so an unauthenticated request carrying no signature passes the check. Processing then continues to postComment, which takes the repository and issue objects directly from the request body, letting the caller direct the deployed function to post a comment on a repository and issue of their choosing using the configured GITHUB_TOKEN, with the issue author login from the body interpolated into the comment text.	2026-08-20	5.8	CVE-2026-72861
ArcadeData--arcadedb	ArcadeDB versions 26.4.2 through 26.7.3 contain an authorization bypass vulnerability in the set_server_setting MCP server-level tool. SetServerSettingTool.execute() gates only on the global allowAdmin flag and never checks the caller's role, so in an MCP deployment with allowAdmin=true and a non-root allowedUsers set, any authenticated read-only user can invoke set_server_setting to modify server GlobalConfiguration, enabling configuration tampering or denial of service. The issue is fixed in 26.8.1.	2026-08-18	6.3	CVE-2026-75845
ArcadeData--arcadedb	ArcadeDB (com.arcadedb:arcadedb-server) versions <= 26.7.3 contain an insecure direct object reference (IDOR) vulnerability in the Raft cluster-info endpoints (GetClusterHandler and PostBootstrapStateHandler), which authenticate but do not authorize access. On an ArcadeDB HA cluster (only reachable when arcadedb.ha.enabled is set and the ha-raft module is loaded), any authenticated user - including one granted access to only one database or none - can enumerate the full server database registry and retrieve per-database metadata such as	2026-08-18	4.3	CVE-2026-75839

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	database names, last transaction IDs, bootstrap fingerprints, and peer/leader cluster topology, resulting in cross-database information disclosure. Fixed in 26.8.1.			
ArcadeData--arcadedb	ArcadeDB before 26.8.1 contains a denial of service vulnerability in the Cypher range() function that allows authenticated users to exhaust server heap memory. Attackers can submit oversized range() expressions with large bounds to trigger OutOfMemoryError and cause temporary service degradation or unavailability.	2026-08-18	4.3	CVE-2026-75841
ArcadeData--arcadedb	ArcadeDB before 26.8.1 fails to bind the authenticated principal (setCurrentUser) on its batch and time-series HTTP handlers. Because no principal is bound on the worker thread, the engine's fine-grained per-type ACL layer (LocalBucket.checkPermissionsOnFile) does not execute for these handlers. In deployments that use per-type or per-group ACLs, a user with database access but only limited per-type permissions can read from and write to types they are not authorized to access by submitting requests to the batch/time-series endpoints. Deployments that rely solely on database-level access control are not affected.	2026-08-18	4.2	CVE-2026-75850
averta--Shortcodes and extra features for Phlox theme	Unauthenticated Sensitive Data Exposure in Shortcodes and extra features for Phlox theme <= 2.17.22 versions.	2026-08-18	5.3	CVE-2026-74008
AWS--Athena Federated Query Clickhouse Connector deployment template	Incorrect privilege assignment in the ClickHouse connector deployment template in Amazon Athena Federated Query prior to v2026.17.1 could allow an authenticated remote user to read arbitrary AWS Secrets Manager secrets in the deploying account by pointing the connector's connection string at an unrelated secret and at a database endpoint under the user's control, causing the connector to transmit the secret to that endpoint. To remediate this issue, users should upgrade to aws-athena-query-federation connectors version v2026.17.1 or later and ensure that any forked or derivative code is patched to incorporate the new fixes. Alternatively, to remediate this issue, users should redeploy the connector with the current template and supply a non-empty SecretNamePrefix value.	2026-08-20	6.5	CVE-2026-75910
axllent--mailpit	Mailpit is an email testing tool and API for developers. From 1.29.0 until 1.30.6, Mailpit's server/server.go origin middleware checks the raw RequestURI for the /api/ prefix while Go's ServeMux routes using the percent-decoded URL path, and server/websockets/client.go configures websocket.Upgrader.CheckOrigin to return true. A malicious website can request /%61pi/events, skip corsOriginAccessControl(), reach the /api/events WebSocket handler, and receive live message IDs, Message-Id values, sender and recipient fields, subjects, tags, and body snippets from an unauthenticated default Mailpit instance after the user visits the site. This is a regression of the earlier WebSocket origin protection and does not affect deployments protected by --ui-auth-file. This issue is fixed in version 1.30.6.	2026-08-20	6.5	CVE-2026-67448
axllent--mailpit	Mailpit is an email testing tool and API for developers. Prior to 1.30.4, Mailpit reads SMTP commands through internal/smtpd/smtpd.go session.readLine() using bufio.Reader.ReadString before session.parseLine() parses the verb or the RFC 5321 512-octet command-line limit is enforced. An unauthenticated remote SMTP client can send an oversized single command line that is fully allocated before syntax rejection or timeout, and the normal MaxMessageSize and DATA limits do not apply to this pre-DATA path. The same command reader is used by handleAuthLogin(), handleAuthPlain(), and handleAuthCramMD5() continuation lines, so concurrent oversized inputs can create memory pressure and reduce service availability. This issue is fixed in version 1.30.4.	2026-08-20	5.3	CVE-2026-67445
axllent--mailpit	Mailpit is an email testing tool and API for developers. Prior to 1.30.4, Mailpit decodes attacker-supplied image attachments into a full raster before checking decoded dimensions, pixel count, or memory use in the GET /api/v1/message/{id}/part/{partID}/thumb endpoint. The Thumbnail handler in server/apiv1/thumbnails.go obtains attachment bytes through storage.GetAttachmentPart(), accepts image/* content, and calls imaging.Decode()	2026-08-20	5.3	CVE-2026-67446

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with AutoOrientation before imaging.Fill() scales the image to 180 by 120 pixels. A compact image declaring very large dimensions can therefore consume disproportionately large memory and CPU, and opening the message UI can trigger the same endpoint through server/ui-src/components/message/MessageAttachments.vue. This can degrade availability when an unauthenticated client can store the crafted attachment and reach the web API. This issue is fixed in version 1.30.4.			
axllent--mailpit	Mailpit is an email testing tool and API for developers. From 1.30.0 until 1.30.5, Mailpit's internal/smtpd/smtpd.go readData() function calls bufio.Reader.ReadBytes before applying the len(data)+len(line) size check to the completed SMTP DATA line against Server.MaxSize. An unauthenticated SMTP client can send a single line larger than the configured MaxMessageSize, causing the full line to be allocated before Mailpit returns the 552 5.3.4 rejection. This post-fix gap remains after normal multi-line DATA accumulation was bounded, and concurrent oversized lines can create substantial memory pressure beyond the configured message-size cap. This issue is fixed in version 1.30.5.	2026-08-20	5.3	CVE-2026-67447
basecamp--trix	Trix is a what-you-see-is-what-you-get rich text editor for everyday writing. Prior to 2.1.17, Trix is vulnerable to cross-site scripting when a data-trix-serialized-attributes attribute bypasses the DOMPurify sanitizer. An attacker can craft HTML containing a data-trix-serialized-attributes attribute with a malicious payload that, when rendered, executes arbitrary JavaScript in the user's session and may perform unauthorized actions or disclose sensitive information. This issue is fixed in version 2.1.17.	2026-08-18	4.6	CVE-2026-73426
bigbluebutton--bigbluebutton	BigBlueButton is an open-source virtual classroom. Prior to 3.0.29, BigBlueButton failed to escape meetingName in record-and-playback/screenshare/playback/index.html.erb when generating the screenshare playback format. A low-privileged user could store a crafted meeting name that embedded script content, and the script executed in another user's browser when that user replayed the recording. This issue is fixed in version 3.0.29.	2026-08-20	5.4	CVE-2026-55491
bigbluebutton--bigbluebutton	BigBlueButton is an open-source virtual classroom. Prior to 3.0.29, BigBlueButton presenters could submit a presentationId through /api/graphql that identified a presentation belonging to another meeting. akka-bbb-apps/src/main/scala/org/bigbluebutton/core/apps/presentationpod/RemovePresentationPubMsgHdlr.scala did not verify the presentation's meeting identifier before deletion, allowing a presenter who knew the identifier to delete another meeting's presentation and disrupt its availability. This issue is fixed in version 3.0.29.	2026-08-20	4.9	CVE-2026-55489
bluwave-labs--Checkmate	Checkmate is an open-source, self-hosted tool designed to track and monitor server hardware, uptime, response times, and incidents in real-time with beautiful visualizations. From 3.5.1 until 3.9.2, an authenticated admin or superadmin can set matchMethod to regex and place a malicious expression in the expectedValue field for advanced HTTP monitor matching. server/src/api/validation/monitorValidation.ts accepts the expression, and server/src/service/network/AdvancedMatcher.ts synchronously evaluates it against an attacker-controlled HTTP response body on the Node.js main event loop without a timeout or worker isolation, allowing catastrophic backtracking to freeze API endpoints, monitor checks, and WebSocket connections for all users. This issue is fixed in version 3.9.2.	2026-08-21	4.9	CVE-2026-70656
Brushfire--Online Experience	The Brushfire platform's video content streaming application (https://online.brushfire.com) exposes database path in requests to users, allowing a remote, unauthenticated attacker to read information about other users. Fixed February 2026.	2026-08-21	5.3	CVE-2026-75928

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
buildwps--PPWP Password Protect Pages	The PPWP: Password Protect Pages, Posts & Full or Partial Content plugin for WordPress is vulnerable to unauthorized access of data due to a improper capability check on the can_access function in all versions up to, and including, 1.9.15. This makes it possible for authenticated attackers, with Contributor-level access and above, to retrieve a master-password and access any password-protected content.	2026-08-18	4.3	CVE-2025-11729
bunkerity--bunkerweb	BunkerWeb is an open-source, next-generation Web Application Firewall. Prior to 1.6.13, the blacklist, greylist, and antibot modules in src/common/core/blacklist/blacklist.lua, src/common/core/greylist/greylist.lua, and src/common/core/antibot/antibot.lua trust PTR suffix matches in IGNORE_RDNS, GREYLIST_RDNS, and ANTIBOT_IGNORE_RDNS without using get_ips to confirm that the hostname resolves to the client address. An unauthenticated remote attacker who controls a PTR record can spoof a trusted suffix to bypass rDNS-based blacklisting, gain greylist treatment, or skip an antibot challenge. This issue is fixed in version 1.6.13.	2026-08-20	5.9	CVE-2026-75514
Canop--broot	broot renders each file and directory name in its interactive tree view exactly as read from the filesystem. Names are converted with a plain to_string_lossy() call in src/tree_build/builder.rs and in TreeLine::unprune in src/tree/tree_line.rs, and no control-character filtering exists anywhere in the code, even though the doc comment on the TreeLine name field states that some characters may have been stripped. Any local user who can create a file can therefore place an escape sequence in its name and have it written unmodified to the terminal of anyone who browses that directory, between broot's own styling codes. A reported proof of concept used an OSC 52 clipboard-write sequence and captured the raw bytes broot wrote to its pty, confirming the sequence reaches the terminal unstripped. What an injected OSC or CSI sequence can then do depends on the terminal emulator in use. Browsing a directory is broot's primary function and carries no expectation that the content is trusted.	2026-08-20	4.6	CVE-2026-72847
cefsharp--CefSharp	CefSharp provides .NET bindings for the Chromium Embedded Framework for Windows Forms and Windows Presentation Foundation applications. Prior to version 148.0.90, CefSharp/SchemeHandler/FolderSchemeHandlerFactory.cs used filePath.StartsWith(rootFolder, StringComparison.OrdinalIgnoreCase) to decide whether a decoded and canonicalized request path remained inside rootFolder. That raw prefix test did not enforce a directory boundary, so a request such as ..%2fwww2/secret.txt could escape a configured www directory into a sibling www2 directory whose path shared the same string prefix. Applications that register FolderSchemeHandlerFactory for a custom scheme or an HTTP or HTTPS scheme can therefore serve local files outside the intended root when an attacker can cause the embedded browser to request the crafted URL. The issue affects both Unix-style paths such as /tmp/app/www2 and Windows paths such as C:\app\www2, and the fix appends a directory separator to the normalized root before comparison while rejecting null bytes and alternate data stream syntax. This issue is fixed in version 148.0.90.	2026-08-18	5.3	CVE-2026-48796
cenocode--CrossWatch	CrossWatch (CW) is a synchronization engine. Prior to version 0.9.21, GET /api/app-auth/status is accessible without authentication and returns the other_sessions array, which exposes metadata of all active sessions - including originating IP addresses, User-Agent strings, internal session IDs, and creation/expiry timestamps. Any unauthenticated network attacker can enumerate this data without credentials. Version 0.9.21 fixes the issue.	2026-08-21	5.3	CVE-2026-53497
cesanta--mongoose	Mongoose is an embedded web server and network library. Prior to 7.22, an attacker who can control an SSI-enabled file can place directory traversal sequences in an #include file or #include virtual directive. The mg_ssi() function in src/ssi.c concatenates the directive argument into a filesystem path without calling mg_path_is_sane(), allowing an MG_ENABLE_SSI deployment with ssi_pattern	2026-08-20	6.5	CVE-2026-73255

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configured to disclose files readable by the Mongoose process. This issue is fixed in version 7.22.			
cesanta--mongoose	Mongoose is an embedded web server and network library. Prior to 7.22, a remote attacker can place a lone carriage return or line feed in multipart input processed by mg_http_next_multipart() in src/http.c. The loops comparing s[b] and s[b + 1], and s[h2] and s[h2 + 1], use an incorrect AND condition and stop when either character resembles part of a CRLF terminator. This truncates headers, filenames, or boundaries and can cause an application to accept dangerous content after seeing a misleading Content-Type value. This issue is fixed in version 7.22.	2026-08-20	6.5	CVE-2026-73258
cesanta--mongoose	Mongoose is an embedded web server and network library. Prior to 7.22, an attacker who can create a file with an HTML payload in its name can trigger stored cross-site scripting when a user browses a directory served with MG_ENABLE_DIRLIST. The printdirentry() path called by listdir() in src/http.c URL-encodes the href but inserts the raw filesystem filename into the HTML link text. The browser executes the injected markup in the Mongoose origin, which can expose session data or permit actions as the victim. This issue is fixed in version 7.22.	2026-08-20	5.4	CVE-2026-73254
cesanta--mongoose	Mongoose is an embedded web server and network library. Prior to 7.22, a remote attacker can send a crafted percent-encoded request path to a deployment using MG_ENABLE_DIRLIST and persuade a user to visit it. The mg_http_serve_dir() and listdir() path in src/http.c places the decoded request URI into the title and h1 elements without HTML entity encoding. The resulting reflected cross-site scripting executes in the Mongoose origin and can expose session data or perform actions as the victim. This issue is fixed in version 7.22.	2026-08-20	5.4	CVE-2026-73259
Charitable--Charitable	The Charitable WordPress plugin before 1.8.12 does not verify the authenticity of incoming Square payment webhook events in a default configuration, allowing unauthenticated attackers to forge webhook notifications that mark donations as paid without any real payment.	2026-08-21	5.3	CVE-2026-16650
CISAgov--Malcolm	Malcolm's upload-processing pipeline (scripts/safe-extract.py) enforces entry-count, nesting-depth, and total-uncompressed-byte limits when extracting container archives (zip/tar/rar/7z via libarchive), but those limits are not applied when the uploaded file is a single-stream compressed format (.gz, .bz2, .xz, .lzma, .lz) that isn't a .tar.*-style archive. Any authenticated user permitted to upload PCAP/log files can upload a small, highly compressible file (e.g. a gzip bomb) that decompresses to an effectively unbounded size on disk, exhausting the shared Docker volume used by OpenSearch, Logstash, Arkime, and Zeek, and disrupting the platform for all users.	2026-08-18	6.5	CVE-2026-19671
CISAgov--Malcolm	Malcolm's nginx Lua role-based access control (RBAC) layer decides whether an authenticated user may reach a role-restricted path (e.g. /htadmin, /auth, /admin_login, /arkime/api/esadmin, NetBox, upload endpoints) by pattern-matching the raw, percent-encoded request URI. Nginx itself, however, selects which location block actually serves the request using the percent-decoded, normalized URI. Because the RBAC check never percent-decodes its input, an authenticated low-privilege user can request an admin-only path using percent-encoding (e.g. /%68tadmin.php) and have nginx route it to the restricted location while the Lua RBAC gate evaluating the un-decoded raw string finds no matching restriction and grants access.	2026-08-18	5.4	CVE-2026-19670
Cisco--Cisco Industrial Ethernet Switches	A vulnerability in the handling of management plane packets by Cisco Industrial Ethernet (IE) 1000 Series Switches could allow an unauthenticated, remote attacker to cause the device manager, SSH, or API to become inaccessible. This vulnerability is due to insufficient protection against management plane flooding attacks. An attacker could exploit this vulnerability by sending a high rate of ICMP, SSH, or HTTP traffic to an affected device. A successful exploit could allow the attacker to cause the CPU of the device to increase, resulting in a denial	2026-08-19	5.3	CVE-2026-20177

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of service (DoS) condition on the device manager web GUI, SSH, or API. Data traffic through the device is not affected.			
Cisco--Cisco Industrial Ethernet Switches	A vulnerability in the web-based management interface of Cisco Industrial Ethernet (IE) 1000 Series Switches could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of another user. To exploit this vulnerability, the attacker must have valid user credentials on the affected system.	2026-08-19	5.4	CVE-2026-20232
Cisco--Cisco Packaged Contact Center Enterprise	A vulnerability in Cisco Packaged Contact Center Enterprise (Packaged CCE) and Cisco Unified Contact Center Enterprise (Unified CCE) could allow an authenticated, remote attacker to conduct server-side request forgery (SSRF) attacks through an affected device. This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device. 	2026-08-19	5	CVE-2026-20314
Cisco--Cisco RoomOS Software	A vulnerability in the USB driver of Cisco RoomOS could allow an unauthenticated, local attacker with physical access to the USB port on an affected device to execute arbitrary code with root privileges. This vulnerability is due to insufficient boundary checks for specific data that is provided through the USB driver. An attacker could exploit this vulnerability by connecting a malicious USB device to an affected device. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected system and execute arbitrary code with root privileges.	2026-08-19	6.1	CVE-2026-20302
Cisco--Cisco Unified Intelligence Center	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an authenticated, local attacker to perform a blind SQL injection attack against an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to read the contents of the internal database of an affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device.	2026-08-19	6.5	CVE-2026-20327
code-projects--Barangay Resident Profiling Management System	A vulnerability was found in code-projects Barangay Resident Profiling Management System 1.0. This impacts an unknown function of the file /archived_records.php of the component Restore/Delete. The manipulation of the argument resident_id results in authorization bypass. The attack may be launched remotely. The exploit has been made public and could be used.	2026-08-23	6.3	CVE-2026-78142
code-projects--Barangay Resident Profiling Management System	A vulnerability was identified in code-projects Barangay Resident Profiling Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /boarders.php of the component Boarder Management Module. Such manipulation of the argument ID leads to authorization bypass. The attack can be executed remotely. The exploit is publicly available and might be used.	2026-08-23	6.3	CVE-2026-78144
code-projects--Login Registration System	A weakness has been identified in code-projects Login Registration System 1.0. This affects an unknown function of the file /loginsystem/database/login_registration_system.sql of the component SQL Database Backup Handler. This manipulation causes files or directories accessible. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-20	5.3	CVE-2026-76799

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Online Shopping System	A weakness has been identified in code-projects Online Shopping System 1.0. Impacted is an unknown function of the file offersmail.php. Executing a manipulation of the argument email can lead to cross site scripting. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2026-08-17	4.3	CVE-2026-19998
CodeAstro--Online Job Portal	A vulnerability was identified in CodeAstro Online Job Portal 1.0. Affected by this vulnerability is an unknown functionality of the file /users/update-profile.php. The manipulation of the argument Name leads to unrestricted upload. The attack can be initiated remotely. The exploit is publicly available and might be used.	2026-08-21	6.3	CVE-2026-77681
CodeCanyon--TimeCamp Integration for CRM	A vulnerability was identified in CodeCanyon TimeCamp Integration for CRM up to 2.8. This issue affects some unknown processing of the file /clients/save_contact of the component Contact Information Update. Such manipulation of the argument contact_id leads to authorization bypass. The attack can be launched remotely. The exploit is publicly available and might be used.	2026-08-17	5.4	CVE-2026-19966
codepeople--Appointment Hour Booking	Unauthenticated Broken Access Control in Appointment Hour Booking <= 1.5.91 versions.	2026-08-18	6.5	CVE-2026-66679
cole--aiosmtplib	aiosmtplib is an asynchronous SMTP client for use with asyncio. Prior to 5.1.2, SMTPProtocol.start_tls in src/aiosmtplib/protocol.py consumes the server's 220 response and starts the TLS handshake without clearing SMTPProtocol._buffer. An active network attacker can place attacker-chosen SMTP response lines after the plaintext 220 response in the same network segment. The method then calls loop.start_tls; those bytes survive the transport upgrade and are parsed as the first response from inside the TLS session, desynchronizing subsequent SMTP command and response pairs. Connections using start_tls=True or opportunistic STARTTLS are affected, while connections using use_tls=True are not. This issue is fixed in version 5.1.2.	2026-08-20	5.9	CVE-2026-55558
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, improper access control in ajax.render.php and ajax.document.php allows for document access without checking on user permissions. This issue has been fixed in version 3.2.3.	2026-08-21	6.5	CVE-2026-34836
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, an unauthenticated user could delete the .readonly file on iTop instances - a file created during the setup process that prevents users from performing write actions. This issue has been fixed in version 3.2.3.	2026-08-21	6.5	CVE-2026-34949
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, the HTML title attribute of the logo in the login page contains the complete iTop version. This issue has been fixed in version 3.2.3.	2026-08-21	5.3	CVE-2026-27463
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, an object can be locked by a user who is not assigned write permissions. This issue has been fixed in version 3.2.3.	2026-08-21	4.3	CVE-2026-33047
COMFAST--CF-N1-S	A security vulnerability has been detected in COMFAST CF-N1-S 2.6.0.1. Impacted is the function sub_44A968 of the file /cgi-bin/mbox-config?method=SET&section=ptest_macaddress. Such manipulation of the argument macaddress leads to command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-17	6.6	CVE-2026-19976
confidential-containers--guest-components	Confidential Containers Guest Components provides guest tools and components for confidential container workloads. From 0.16.0 until 0.20.0, a crafted OCI image layer can make image_rs::stream::unpack::unpack() create a hardlink outside its destination directory. In image-rs/src/stream/unpack.rs, try_hardlink_fallback() validates the hardlink source but computes the destination with	2026-08-18	6.4	CVE-2026-47699

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	destination.join(&entry_rel). Rust Path::join replaces the base when entry_rel is an absolute tar entry path, so fs::hard_link(&src_canon, &dst_entry_abs) can write attacker-controlled content to an arbitrary absolute path. In Confidential Containers the workload owner already controls trusted image content, so the issue is a workload-owner escape into the pod virtual machine rather than a crossing of the image trust boundary, but it may enable access to pod virtual machine capabilities and attestation abuse. This issue is fixed in version 0.20.0.			
containers--buildah	Buildah is a tool that facilitates building OCI images. From 1.38.1 until 1.43.2 and 1.44.0, TempDirForURL in define/types.go does not securely confine Git repository subdirectories to the downloaded build context, and downloadToDirectory and stdinToDirectory can follow a Dockerfile symlink left by a partially extracted tar archive. A malicious server supplying a Git repository or tar archive can cause files outside the build context directory to be included in the context or copied into the build. This issue is fixed in versions 1.43.2 and 1.44.0.	2026-08-21	6.3	CVE-2026-44517
coturn--coturn	Coturn is a free open source implementation of TURN and STUN Server. In 4.15.0, an authenticated TURN user can repeatedly resume one allocation from fresh UDP 5-tuples without completing a handoff when the server enables --mobility. mobile_begin_transition() in src/server/ns_turn_server.c disarms each new session's allocation timeout and overwrites the allocation's single mobile_pending_resume link, leaving earlier pending sessions unreachable by the cleanup path, while copy_auth_parameters() ignores inc_quota() failure. The attacker can therefore retain unbounded server-side sessions and exhaust process memory even when --user-quota=1 is configured. This issue is fixed in version 4.16.0.	2026-08-19	6.5	CVE-2026-68555
coturn--coturn	Coturn is a free open source implementation of TURN and STUN Server. Prior to 4.15.0, an unauthenticated remote client can send a STUN message over TCP or TLS with a body-length field from 65520 through 65532, causing the uint16_t len variable in stun_get_message_len_str() in src/client/ns_turn_msg.c to wrap when STUN_HEADER_LENGTH is added. The framing layer then consumes only 4 through 16 bytes, treats the remaining bytes as another message, desynchronizes the stream parser, and drops the attacking client's connection. Other clients and the server process are not affected. This issue is fixed in version 4.15.0.	2026-08-19	5.3	CVE-2026-68552
CTFd--CTFd	A vulnerability has been found in CTFd up to 3.8.4. The affected element is the function _is_safe_url of the file CTFd/utlis/validators/__init__.py. Such manipulation of the argument Next leads to open redirect. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 5d8515842fd1ab2c3a9f2dde9ffca907aa334ea9. Upgrading the affected component is recommended.	2026-08-23	4.3	CVE-2026-78145
David Artiss--Draft List	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Artiss Draft List simple-draft-list allows Stored XSS. This issue affects Draft List: from n/a through 2.6.4.	2026-08-18	6.5	CVE-2026-66603
David Lingren--Media Library Assistant	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David Lingren Media Library Assistant allows Stored XSS. This issue affects Media Library Assistant: from n/a through 3.39.	2026-08-18	6.5	CVE-2026-66591
David Lingren--Media Library Assistant	Subscriber Cross Site Scripting (XSS) in Media Library Assistant <= 3.39 versions.	2026-08-20	6.5	CVE-2026-66601
DeDeCMS--DeDeCMS	A flaw has been found in DeDeCMS 3. Affected by this vulnerability is an unknown functionality of the file /include/dialog/select_media_post.php. Executing a manipulation of the argument uploadfile can lead to unrestricted upload. The attack can be executed remotely. The exploit has been published and may be used.	2026-08-20	6.3	CVE-2026-76800

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Deepen Bajracharya--Video Conferencing with Zoom	Contributor Cross Site Scripting (XSS) in Video Conferencing with Zoom <= 4.6.8 versions.	2026-08-18	6.5	CVE-2026-66641
Dell--Alienware Command Center (AWCC)	Dell Alienware Command Center (AWCC), versions prior to 6.14.20.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of Service and Elevation of Privileges.	2026-08-18	6	CVE-2026-49500
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-08-19	6.6	CVE-2026-56796
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges and Server-side request forgery.	2026-08-19	6.5	CVE-2026-67268
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain an Incorrect Authorization vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-08-19	5.5	CVE-2026-67266
Dell--Dell Command Update (DCU)	Dell Command Update (DCU), versions prior to 5.7.1, contain an Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2026-08-19	5.5	CVE-2026-67267
Dell--ObjectScale	Dell ObjectScale, versions prior to 4.3.0.1, contain(s) an Insertion of Sensitive Information into Log File vulnerability in the svc_tools. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2026-08-17	5.5	CVE-2026-59911
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-08-19	6.5	CVE-2026-70423
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-08-19	6.5	CVE-2026-70424
Dell--OpenManage Enterprise	Dell OpenManage Enterprise, versions prior to 4.7.0, contains an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-08-19	4.6	CVE-2026-54793
Dell--PowerPath	Dell PowerPath, version 7.2 through to 8.0 SP1, contains an Improper Privilege Management vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-08-19	5.3	CVE-2026-32802
deskflow--deskflow	Deskflow is a keyboard and mouse sharing app. From 1.17.0 until continuous build 1.26.0.300, a connected peer can send repeated DCLP DataChunk messages to ClipboardChunk::assemble() in src/lib/deskflow/ClipboardChunk.cpp, causing the server path in src/lib/server/ClientProxy1_6.cpp or client path in src/lib/client/ServerProxy.cpp to append data beyond the DataStart declared size and configured clipboard limit before DataEnd validation, exhausting receiver memory. This issue is fixed in continuous build 1.26.0.300.	2026-08-17	6.5	CVE-2026-65976
dicebear--dicebear	DiceBear is an avatar library for designers and developers. Prior to 9.4.3, @dicebear/core interpolates the rotate option into an SVG transform attribute	2026-08-20	4.7	CVE-2026-68921

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	without XML escaping in addRotate in packages/@dicebear/core/src/utls/svg.ts, while @dicebear/initials similarly emits fontSize and fontWeight without escaping in packages/@dicebear/initials/src/index.ts. Runtime callers can pass strings despite the numeric TypeScript types, break out of the attributes, and inject arbitrary SVG markup. Script can execute in the page origin when the generated avatar is inserted inline or served as image/svg+xml and opened directly, although exploitation requires an application to pass untrusted values into these normally developer-controlled options. This issue is fixed in @dicebear/core and @dicebear/initials version 9.4.3.			
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, hidden or otherwise unviewable first-post content was leaked as an excerpt in the publicly-served Q&A (QAPage) JSON-LD structured data, exposing it to any unauthenticated visitor and to search-engine crawlers. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-17	5.3	CVE-2026-53960
discourse--discourse	Discourse is an open-source discussion platform. Prior o 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0, users who were allowed to view a group's activity, but were not permitted to see shared drafts, could still receive shared-draft entries through the group posts and group mentions endpoints. This could disclose shared-draft topic titles and post excerpt/content, resulting in an information disclosure of unpublished draft material. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.0.	2026-08-17	4.3	CVE-2026-55704
discourse--discourse	Discourse is an open-source discussion platform. Prior to 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.1, on sites with category group moderation enabled, the review queue could include an excerpt (and permalink) of the private message attached to a flag, even when the reviewing category moderator was not a participant in that message. These notify_moderators flag messages are addressed only to moderators and, for core flags, to a category's moderation groups as they existed when the flag was raised, so a category group moderator could read flag-discussion content they were not authorized to see. This affects official plugins that create such messages and core flags raised before a moderator's group was granted moderation of the category. Only the confidentiality of a limited excerpt of these flag-related private messages is affected; no content can be modified or deleted. This issue is fixed in versions 2026.1.6, 2026.5.2, 2026.6.1, and 2026.7.1.	2026-08-17	4.3	CVE-2026-59829
django-cms--django-cms	django CMS is an easy-to-use and developer-friendly enterprise content management system powered by Django. Prior to 5.0.8, the copy_plugins endpoint in cms/admin/placeholderadmin.py authorizes only the destination clipboard. The _copy_plugin_to_clipboard and _copy_placeholder_to_clipboard paths accept source_placeholder_id and source_plugin_id values but use has_copy_plugins_permission and check_source only for the requesting user's clipboard, without validating the source placeholder. Under CMS_PERMISSION, a staff user with the global add permission for a plugin type can copy plugins from an unauthorized page or placeholder into the user's clipboard and read secret text, link names, and URLs. This issue is fixed in versions 5.0.8.	2026-08-20	6.5	CVE-2026-54622
django-cms--django-cms	django CMS is an easy-to-use and developer-friendly enterprise content management system powered by Django. Prior to 5.0.8, render_object_structure in cms/views.py renders cms/toolbar/structure.html for a PageContent object without calling user_can_view_page(). Any staff account can request a restricted page's structure when CMS_PERMISSION is enabled and the page has view restrictions or CMS_PUBLIC_FOR is set to staff. The response exposes plugin get_short_description() values, including link names, URLs, and text snippets, rather than only the page shape. This issue is fixed in versions 5.0.8.	2026-08-20	6.5	CVE-2026-54624
django-cms--django-cms	django CMS is an easy-to-use and developer-friendly enterprise content management system powered by Django. Prior to 5.0.9, page duplication lacks an object-level authorization check on the source page. In cms/admin/forms.py, DuplicatePageForm.source accepts any Page, the AddPageForm constructor does	2026-08-20	6.5	CVE-2026-63003

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	not narrow a hidden source field, AddPageForm.clean does not validate the source against the user, and AddPageForm.save calls from_source. In cms/admin/pageadmin.py, duplicate and PageAdmin.has_add_permission check only whether a staff user may add a page. A crafted source value can therefore copy every placeholder and plugin from an unauthorized page with permissions=False, stripping source view restrictions and exposing content across sites or restricted subtrees when CMS_PERMISSION is enabled. This issue is fixed in versions 5.0.9.			
django-cms-- django-cms	django CMS is a content management system powered by Django. Prior to 5.0.8 and in 5.1.0a1, the django CMS page cache in cms/cache/page.py ignores request headers declared by plugins through get_vary_cache_on(). The _page_cache_key function includes the cache prefix, site, language, path, and timezone but not the declared header values. Although set_page_cache adds those names to the response Vary header, get_page_cache retrieves the first stored variant under the same header-agnostic key. When CMS_PAGE_CACHE is enabled and a plugin varies content on a header such as Country-Code, one visitor can receive another visitor's request-specific content, and an unauthenticated attacker can prime the cache with attacker-chosen content. This issue is fixed in versions 5.0.8 and 5.1.0.	2026-08-20	4.8	CVE-2026-54625
django-cms-- django-cms	django CMS is an easy-to-use and developer-friendly enterprise content management system powered by Django. Prior to 5.0.9, render_object_structure fails to authorize non-PageContent objects that use PlaceholderRelationField. An active staff user without cms.use_structure or model-level view or change permission can request the //admin/cms/placeholder/object/<content_type_id>/structure/<object_id>/ endpoint with guessed content_type_id and object_id values. The response discloses placeholder slot names, plugin trees, plugin identifiers, labels, and object existence for frontend-editable objects. The fix applies user_can_view_placeholder_source to the non-PageContent branch while keeping the structure board read-only for view-only users. This issue is fixed in versions 5.0.9.	2026-08-20	4.3	CVE-2026-61663
django-cms-- django-cms	django CMS is an easy-to-use and developer-friendly enterprise content management system powered by Django. From 5.0.8 until 5.0.9, ContentRenderer.render_placeholder in cms/plugin_rendering.py can pass stored, attacker-controlled values to ContentRenderer.render_exception when plugin rendering fails in edit mode. Values from get_short_description(), the exception message, the placeholder, or placeholder.source are interpolated into a cms-rendering-exception heading and later returned through mark_safe. Because the heading is not escaped, stored HTML executes in an editor's browser, and settings.DEBUG does not prevent the custom heading from rendering. The fix uses format_html to escape the message before safe placeholder output is returned. This issue is fixed in versions 5.0.9.	2026-08-20	4.4	CVE-2026-75526
Dokploy--dokploy	Dokploy is a free, self-hostable Platform as a Service (PaaS). Prior to 0.29.6, Dokploy's user.update procedure in apps/dokploy/server/api/routers/user.ts updates account.password without deleting other rows from session, allowing a compromised better-auth.session_token session to remain valid for up to three days after a password change. This issue is fixed in version 0.29.6.	2026-08-17	5.9	CVE-2026-45791
Dolibarr--Dolibarr	A weakness has been identified in Dolibarr up to 23.0.4. This affects an unknown part of the file htdocs/user/card.php of the component Account Handler. This manipulation of the argument ID causes improper authorization. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 24.0.0 is able to mitigate this issue. Patch name: b2a2c995537cb6282383b5e903cb5ffa29b823e6. The affected component should be upgraded.	2026-08-21	5.4	CVE-2026-77686
drakkan--sftpgp	SFTPGO is an open source, event-driven file transfer solution. From 2.2.0 until 2.7.3, the public web-client partial ZIP download endpoint for a browsable share	2026-08-20	5.9	CVE-2026-49244

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	validates client-supplied files entries with a raw byte-prefix comparison rather than a directory-boundary-aware check. An unauthenticated requester who can reach a public share can select a canonical path outside the shared directory when the target path begins with the shared directory's name, such as a sibling path that shares the same prefix. The endpoint then includes the out-of-scope file in the generated download, disclosing its contents. This issue is fixed in version 2.7.3.			
Dromara--RuoYi-Vue-Plus	A vulnerability was identified in Dromara RuoYi-Vue-Plus up to 5.6.2. This issue affects the function FlwInstanceController/FlwDefinitionController/FlwCategoryController/FlwSpelController/TestLeaveController of the component Workflow Endpoint. Such manipulation leads to improper authorization. The attack can be launched remotely.	2026-08-21	6.3	CVE-2026-77795
Dromara--UJCMS	A flaw has been found in Dromara UJCMS up to 10.1.3. The impacted element is the function update of the file src/main/java/com/ujcms/cms/ext/web/backendapi/WebFileTemplateController.java of the component web-file-template Endpoint. Executing a manipulation can lead to improper neutralization of special elements used in a template engine. The attack can be launched remotely. The exploit has been published and may be used.	2026-08-23	4.7	CVE-2026-78140
dvankooten--MC4WP: Mailchimp for WordPress	The MC4WP: Mailchimp for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form response message post meta fields (e.g., 'text_subscribed', 'text_error') in all versions up to, and including, 4.12.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-22	6.4	CVE-2026-4561
eidetic-labs--stigmeme-node	Stigmeme before 0.9.0a11 fails to validate the delivery_address parameter when creating webhook subscriptions, allowing authenticated users to specify internal loopback and private network destinations. Attackers can trigger matching fact-change events to cause the Stigmeme server to issue server-side HTTP POST requests to internal services, enabling blind SSRF attacks against localhost and private network endpoints.	2026-08-19	6.3	CVE-2026-76239
elunez--eladmin	A vulnerability was found in elunez eladmin up to 2.7. The impacted element is the function EmailController/AlipayController/GeneratorController/GenConfigController. The manipulation results in improper authorization. The attack can be launched remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-20	6.3	CVE-2026-77036
EmilStenstrom--justhtml	justhtml versions before 1.13.0 contain a cross-site scripting vulnerability in the to_markdown() function when serializing attacker-controlled pre content. Attackers can place backticks inside sanitized pre elements to break out of fixed-length code fences, allowing raw HTML to execute when the generated Markdown is rendered by CommonMark or GFM-style renderers.	2026-08-23	6.1	CVE-2026-5389
EmilStenstrom--justhtml	justhtml versions 1.13.0 and earlier contain a parser-differential / mutation cross-site scripting (mXSS) vulnerability when using a custom SanitizationPolicy that preserves foreign namespaces (e.g., drop_foreign_namespaces=False with allowlisted SVG/MathML elements or raw-text containers such as <style>). Specially crafted input can sanitize into markup that appears safe but becomes unsafe when re-parsed by a browser or another HTML parser, allowing markup injection. The default safe configuration (sanitize=True) is not affected. Fixed in 1.14.0.	2026-08-23	6.1	CVE-2026-5751
EmilStenstrom--justhtml	justhtml before 1.17.0 contains multiple security issues in sanitization, serialization, and programmatic DOM handling. When custom policies preserve foreign namespaces (SVG/MathML), dangerous content such as HTML integration points (SVG <foreignObject>, MathML <annotation-xml encoding="text/html">) and	2026-08-23	6.1	CVE-2026-6827

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mutation-XSS parser-differential payloads could survive sanitization and become active HTML after reparse; SVG filter="url(...)" and preserved <style> could leave resource-loading CSS (@import, background-image:url()). Programmatic script/style/Comment nodes could serialize into active markup. Additional hardening fixes address sanitize-pipeline cache mutation and DOM parent/child cycles that could cause infinite loops. Most issues affect advanced or custom configurations rather than the default JustHTML(..., sanitize=True) safe path.			
EmilStenstrom--justhtml	justhtml before 3.11.0 contains a cross-site scripting vulnerability where the default sanitizer bypasses event handler removal in selectedcontent projections. Attackers can inject SVG or MathML elements with event handlers that are cloned and reinserted into output without sanitization, enabling stored or reflected XSS attacks.	2026-08-23	6.1	CVE-2026-74793
EmilStenstrom--justhtml	justhtml versions 0.9.0 through 1.21.0 contain a cross-site scripting vulnerability in to_markdown() where inline code spans fail to account for blank lines as block boundaries. Attackers can inject blank lines into code or pre element text to break the inline span, causing sanitized HTML to be emitted unescaped and re-parsed as live Markdown by compliant renderers.	2026-08-23	6.1	CVE-2026-77088
EmilStenstrom--justhtml	justhtml before 1.12.0 (versions <= 1.11.0) contains a mutation cross-site scripting (mXSS) vulnerability in the serialization of raw-text elements such as <style> and <script>. When a DOM tree is processed by sanitize_dom() using a custom policy that keeps these elements, text nodes inside them are serialized literally without escaping, allowing attacker-controlled text containing the matching closing tag sequence to break out of the raw-text context and inject arbitrary HTML into the serialized output. The default sanitization policy is not affected because it drops the contents of style and script.	2026-08-23	6.1	CVE-2026-8630
emqx--emqx	EMQX is a scalable and reliable MQTT broker for AI, IoT, IIoT, and connected vehicles. Prior to versions 5.8.11, 5.9.3, 5.10.4, 6.0.3, 6.1.2, and 6.2.1, the plugin-install REST API and dashboard upload accepted stale grants created with emqx ctl plugins allow because there was no five-minute grant lifetime or SHA-256 package binding. An attacker with a compromised dashboard administrator credential or API key with plugin-install permission who finds a stale allowed name and version can upload attacker-controlled bytes under the allowed .tar.gz filename through POST /api/v5/plugins/install or the dashboard plugin upload. The broker then installs and runs attacker-controlled Erlang code with the privileges of the EMQX process. This issue is fixed in versions 5.8.11, 5.9.3, 5.10.4, 6.0.3, 6.1.2, and 6.2.1.	2026-08-20	6.6	CVE-2026-44725
EricLBuehler--Mistral.rs	A vulnerability was detected in EricLBuehler Mistral.rs up to 0.8.22. Affected by this issue is the function convert_gguf_to_hf_tokenizer of the file mistralrs-core/src/gguf/gguf_tokenizer.rs of the component GGUF Tokenizer. The manipulation of the argument eos_token_id/bos_token_id/unknown_token_id results in out-of-bounds read. The attack can be executed remotely. The exploit is now public and may be used. Upgrading to version 0.8.23 can resolve this issue. The patch is identified as cd5297e2ea5cb27c790bdcf2f3c2f1064a81d55e. Upgrading the affected component is recommended.	2026-08-18	4.3	CVE-2026-75090
Esri--Portal for ArcGIS	There is a reflected cross site scripting vulnerability in Esri Portal for ArcGIS versions 11.5 and prior which may allow a remote, unauthenticated attacker to create a crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. Users working with ArcGIS Enterprise 11.1, 11.3, and 11.5 are encouraged to patch. All users are advised to upgrade to the latest long-term support release. Users working with ArcGIS Web App Builder developer edition are advised to migrate to ArcGIS Experience Builder, as ArcGIS Web App Builder developer edition is unsupported when this CVE is assigned.	2026-08-21	6.1	CVE-2026-69234
Esri--Portal for ArcGIS	There is a stored cross site scripting issue in Esri Portal for ArcGIS versions 11.5 and prior that may allow a remote, privileged attacker to inject malicious code that could potentially execute arbitrary in a victim's browser. Users working with ArcGIS	2026-08-21	6.1	CVE-2026-69235

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Enterprise 11.1, 11.3, and 11.5 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.			
Esri--Portal for ArcGIS	There is a stored cross site scripting issue in Esri Portal for ArcGIS versions 12.1 and prior that may allow a remote, privileged attacker to inject malicious code that could potentially execute arbitrary JavaScript in a victim's browser. Users working with ArcGIS Enterprise 11.1, 11.3, 11.5, 12.0 or 12.1 are encouraged to patch. All users are advised to upgrade to the latest long-term support release and apply the patch.	2026-08-21	6.1	CVE-2026-69236
Esri--Portal for ArcGIS	There is an information disclosure vulnerability in Esri Portal for ArcGIS versions 12.0 and earlier that may under difficult to reproduce circumstances allow a remote, unauthenticated attacker to reflect sensitive information in a http response body.	2026-08-21	5.9	CVE-2026-69224
Esri--Portal for ArcGIS	There is an information disclosure vulnerability in Esri Portal for ArcGIS versions 11.5 through 12.0 and earlier that may allow a remote, unauthenticated attacker to reflect sensitive information in a http response body.	2026-08-21	5.9	CVE-2026-69225
Esri--Portal for ArcGIS	There is a missing authentication vulnerability in Esri Portal for ArcGIS versions 12.0 and prior that may allow a remote, unauthenticated attacker to access a specific resource (not user content) that should only be accessible by authenticated users. Users working with ArcGIS Enterprise 11.1, 11.3, 11.5, or 12.0 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.	2026-08-21	5.3	CVE-2026-69228
Esri--Portal for ArcGIS	There is an HTML injection vulnerability in Esri Portal for ArcGIS versions 12.0 and prior that allows a remote, authenticated attacker to insert arbitrary HTML into the Portal for ArcGIS Home application. Users working with ArcGIS Enterprise 11.1, 11.3, 11.5 and 12.0 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.	2026-08-21	5.4	CVE-2026-69229
Esri--Portal for ArcGIS	There is a stored cross site scripting issue in Esri Portal for ArcGIS versions 11.5 and prior that may allow a remote, administratively privileged attacker to inject malicious code that could potentially execute arbitrary in a victim's browser. Users working with ArcGIS Enterprise 11.1, 11.3, and 11.5 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.	2026-08-21	5.5	CVE-2026-69230
Esri--Portal for ArcGIS	There is a stored cross site scripting issue in Esri Portal for ArcGIS versions 11.5 and prior that may allow a remote, privileged attacker to inject malicious code that could potentially execute arbitrary JavaScript in a victim's browser. Users working with ArcGIS Enterprise 11.1, 11.3, 11.5 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.	2026-08-21	5.5	CVE-2026-69231
Esri--Portal for ArcGIS	There is a stored cross site scripting issue in Esri Portal for ArcGIS versions 11.5 and prior that may allow a remote, privileged attacker to inject malicious code that could potentially execute arbitrary JavaScript in a victim's browser. Users working with ArcGIS Enterprise 11.1, 11.3, 11.5 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.	2026-08-21	5.5	CVE-2026-69232
Esri--Portal for ArcGIS	There is a stored cross site scripting issue in Esri Portal for ArcGIS versions 11.5 and prior that may allow a remote, administratively privileged attacker to inject malicious code that could potentially execute arbitrary in a victim's browser. Users working with ArcGIS Enterprise 11.1, 11.3, and 11.5 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.	2026-08-21	5.5	CVE-2026-69233
ether--etherpad	Etherpad is a real-time collaborative editor. From 2.1.0 until 3.1.0, Etherpad uses the attacker-controlled x-proxy-path request header in src/node/hooks/express/admin.ts when substituting paths into HTML, JavaScript, and CSS under /admin without sanitization, Vary: x-proxy-path, or Cache-Control: private, no-store. A shared proxy or CDN can cache the resulting response and serve attacker-injected script to an administrator. In src/node/hooks/express/specialpages.ts, version 3.0.0 also accepts a protocol-	2026-08-19	6.1	CVE-2026-55087

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	relative x-proxy-path value when constructing the /p/:pad/timeslider redirect, allowing redirection to an attacker-controlled host. The issues are exploitable when the deployment permits client-supplied x-proxy-path headers to reach Etherpad. This issue is fixed in version 3.1.0.			
ether--etherpad	Etherpad is a real-time collaborative editor. From 2.6.0 until 3.1.0, Etherpad's src/node/hooks/express/tokenTransfer.ts uses POST /tokenTransfer to store an author token for transfer between browsers and exposes it through GET /tokenTransfer/{uuid}. Although the record includes createdAt, the transfer has no expiration check, is not removed after successful redemption, and is returned by res.send(tokenData), including the raw author token. An unauthenticated attacker who obtains a transfer UUID can repeatedly redeem it, receive fresh author cookies, read the cleartext token, and impersonate the originating author for pad read and write operations. This issue is fixed in version 3.1.0.	2026-08-19	6.8	CVE-2026-55088
ether--etherpad	Etherpad is a real-time collaborative editor. Prior to 3.1.0, src/node/handler/ImportHandler.ts and src/node/handler/ExportHandler.ts derive temporary filenames from Math.random() and place them in os.tmpdir(). On a host with a shared world-writable temporary directory, a local unprivileged attacker who predicts a filename can precreate a symbolic link to a file writable by the Etherpad process. Subsequent import or export operations can follow the link through fs.writeFile, fs.rename, or document-conversion output and overwrite the target with partially attacker-controlled content. This issue is fixed in version 3.1.0.	2026-08-19	4.2	CVE-2026-55086
fastify--fastify	fastify is a fast and low overhead web framework for Node.js. Impact: the fix for CVE-2026-3635 added a guard on the forwarded-header reads used to derive the request host, protocol, hostname, ip, and ips values, checking the connecting address. That guard closes the IP, CIDR, and custom-function forms of trustProxy correctly, because those forms compile to predicates that inspect the connecting address. The hop-count form, where trustProxy is set to a number, compiles to a predicate that structurally ignores the address, so the guard is always satisfied for any hop count of one or more. Applications configured with a numeric trustProxy value, such as trustProxy set to 1 for a single reverse proxy, remain vulnerable: an attacker who can reach the Fastify origin directly, bypassing the front-facing proxy, can spoof the forwarded request fields exactly as in the unpatched version. The impact class matches the parent CVE-2026-3635, including host injection in generated URLs, HTTPS-enforcement bypass, secure-cookie and CSRF-origin bypass, and host-based routing and cache poisoning. Affected versions are fastify from 5.8.3 up to but not including 5.12.1. Patches: patched in fastify 5.12.1, where the numeric form of trustProxy is disabled at runtime and removed from the TypeScript type union. Workarounds: migrate to an IP, CIDR, or custom-function trustProxy value that validates the connecting address, and ensure the Fastify origin is only reachable through the trusted proxy chain.	2026-08-18	6.1	CVE-2026-16732
fastify--fastify	fastify is a fast and low overhead web framework for Node.js. Versions of fastify before 5.12.1 are affected by a schema validation bypass when a request body schema targets a root primitive value. When the schema validates a top-level primitive such as an integer, Ajv can coerce a JSON string into the expected type during validation, but Fastify does not replace the root request body with the coerced value, so the route handler receives the original unvalidated string. As a result, a request that should have failed validation can reach application logic with a value that does not satisfy the schema, which can undermine integrity and access-control checks that rely on the validated type. Users should upgrade to fastify 5.12.1, which fixes the mismatch. No known workarounds are available.	2026-08-18	5.4	CVE-2026-18504
fbeta-GmbH--ePA3-Service-OpenSource	ePA 3.x Integration implements the authorization workflow and writes Medical Information Objects to Germany's electronic patient record. Prior to 1.3.0, ePA 3.x Integration does not neutralize CRLF characters in values used by app/vau/VAUProtokoll.py to construct VAU inner HTTP requests. The build_inner_header function interpolates the uri, host, accept_type, content_type, content_length, USER_AGENT, and insurant_id values into request lines and	2026-08-18	6.8	CVE-2026-50576

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	headers, including x-useragent and x-insurantid. An authenticated attacker who controls a value can inject additional headers into the inner request. Depending on ePA server handling, an injected x-insurantid header can expose another patient's records, and injected Authorization headers can bypass the intended authentication or authorization context. Session-derived USER_AGENT input can also poison requests across the session. This issue is fixed in version 1.3.0.			
FFmpeg--FFmpeg	FFmpeg before commit b4c199c contains an incorrect integer narrowing conversion in the AV1 RTP packetizer (libavformat/rtpenc_av1.c). The OBU size is cast to long before comparison against the remaining frame size. On targets where long is 32 bits, including 64-bit Windows, sufficiently large OBU size values are sign-flipped by the narrowing cast, producing a negative value that passes the payload size check. This allows an oversized OBU to bypass the safety bound on affected platforms, leading to out-of-bounds memory access when the oversized value is subsequently used as a copy length.	2026-08-19	5.8	CVE-2026-75145
Fileorbis Informatics Services Trade Inc.-FileOrbis	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Fileorbis Informatics Services Trade Inc. FileOrbis allows Stored XSS. This issue affects FileOrbis: before 16.5.	2026-08-18	5.4	CVE-2026-19447
flutterwave--Flutterwave WooCommerce	Unauthenticated Broken Authentication in Flutterwave WooCommerce <= 3.3.0 versions.	2026-08-18	6.5	CVE-2026-73399
forem--forem	Forem is open source software for building communities. In versions before commit 92eacd16a82cf9007ba8e16a2258b42e3b53ca9c, a malicious value submitted through feedback_message[message] is stored without sanitization and rendered in app/views/admin/feedback_messages/_feedback_message.html.erb through raw(feedback_message.message) when offender_id is present. Viewing the abuse report executes arbitrary JavaScript in an administrator's browser and may expose sensitive in-page data, abuse CSRF tokens, or perform administrative actions in the victim's session. The public FeedbackMessagesController accepts the report without authorization and previously permitted a submitted offender_id, making the vulnerable rendering path reachable by an unauthenticated attacker. This issue is fixed in commit 92eacd16a82cf9007ba8e16a2258b42e3b53ca9c	2026-08-18	6.3	CVE-2026-61696
frangoteam--FUXA	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. Prior to 1.3.2, POST /api/scheduler and DELETE /api/scheduler in server/api/scheduler/index.js do not consistently enforce authJwt.haveAdminPermission for scheduler settings. An authenticated non-admin operator can create or alter deviceActions that invoke onSetValue or onRunScript, or delete schedules, gaining access to device-value changes and server-side project script execution normally reserved for administrators. Scheduled and repeating actions can continue changing PLC setpoints, safety interlocks, device state, or project data after the operator's session ends. This issue is fixed in version 1.3.2.	2026-08-18	6.3	CVE-2026-47721
frangoteam--FUXA	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. Prior to 1.3.2, the TDengine DAQ storage connector's escapeTdString function in server/runtime/storage/tdengine/index.js doubles single quotes but does not escape backslashes. A remote unauthenticated attacker can submit a crafted sids tag identifier through GET /api/daq or the Socket.IO DAQ_QUERY event so TDengine interprets the backslash and quote sequence as SQL syntax. The injected query can return every row from fuxa.meters, exposing historical PLC tag values, device identifiers, and device names even when FUXA authentication is enabled. This issue is fixed in version 1.3.2.	2026-08-18	5.3	CVE-2026-47720
Frauscher Sensortechnik--FDS 102	A low privileged remote attacker with a valid session can submit a request to the user creation functionality exposed through /api/user/add.php to create new accounts with arbitrary role values, including the highest privilege level used by the application.	2026-08-20	6.5	CVE-2026-14949

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Frauscher Sensortechnik--FDS 102	A low-privileged remote attacker can enumerate all configured users and identify which accounts hold elevated privileges using the endpoint /api/user/fetch-all.php.	2026-08-20	4.3	CVE-2026-14953
FreeRDP--FreeRDP	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.28.0, an authenticated RDP client can advertise DVI ADPCM with nBlockAlign equal to 8 and nChannels equal to 2 to make the 'bs' calculation in rdpnd_server_select_format in channels/rdpsnd/server/rdpsnd_main.c equal zero. The subsequent out_frames modulo 'bs' operation raises SIGFPE and terminates the server-side rdpsnd channel process. This vulnerability fixed in 3.28.0.	2026-08-19	6.5	CVE-2026-63117
FreeRDP--FreeRDP	FreeRDP is a free implementation of the Remote Desktop Protocol. Prior to 3.27.0, the glyph_cache_get function in libfreerdp/cache/glyph.c checks whether index is greater than cache->number instead of greater than or equal to it. A malicious RDP server can use GLYPH_FRAGMENT_USE replay in update_process_glyph_fragments to make the default cache receive index 254 when cache->number is 254, reading one pointer beyond the entries array and dereferencing it as a glyph. This can crash the client and may disclose adjacent heap data. This issue is fixed in version 3.27.0.	2026-08-19	5.4	CVE-2026-55564
FreeRTOS--FreeRTOS-Kernel	Missing queue-set type validation in xQueueAddToSet() in the FreeRTOS-Kernel before 11.3.1 might allow an unprivileged task on MPU-enabled ports with configUSE_QUEUE_SETS=1 to read privileged kernel memory. To remediate this issue, users should upgrade to version 11.3.1 or later.	2026-08-21	6.5	CVE-2026-77237
froxlor--froxlor	Froxlor is open source server administration software. Prior to 2.3.8, the standalone lib/ajax.php entry point bypasses the centralized request validation in lib/init.php, and Ajax::handle in lib/Froxlor/Ajax/Ajax.php checks only for a valid session before routing state-changing requests. The editapikey action in Ajax::editApiKey updates allowed_from and valid_until without validating a CSRF token, while templates/Froxlor/assets/js/jquery/apikeys.js sends no token because the endpoint does not require one. An unauthenticated attacker can induce an authenticated administrator's browser to submit a forged request that adds an attacker-controlled address to an API key's allowed_from list or removes its expiration, weakening the key's security restrictions. This issue is fixed in version 2.3.8.	2026-08-18	6.5	CVE-2026-55593
froxlor--froxlor	Froxlor is open source server administration software. Prior to 2.3.8, the DomainZones.add API command in lib/Froxlor/Api/Commands/DomainZones.php accepts user-controlled record and type values without rejecting line delimiters, tab characters, semicolons, or unsupported DNS record types before lib/Froxlor/Dns/DnsEntry.php serializes the values into a BIND zone file. An authenticated customer with DNS-zone permissions can place a crafted value in the record field, or use the related type-field variant, to create additional resource-record lines that bypass Froxlor's field-level validation. BIND accepts the injected records, allowing modification of DNS data and possible DNS availability impact within a zone the caller is authorized to manage. This issue is fixed in version 2.3.8.	2026-08-18	5.4	CVE-2026-54543
getgrav--grav	Grav is a file-based Web platform. Prior to 2.0.1, Grav ZipArchiver::extract() in system/src/Grav/Common/Filesystem/ZipArchiver.php passes archives to ZipArchive::extractTo() without enforcing the system.gpm.archive uncompressed-size, file-count, or nesting-depth limits. Code using Archiver::create('zip') to extract an attacker-controlled archive can exhaust disk space or inodes and make the site unavailable. This issue is fixed in version 2.0.1.	2026-08-19	6.5	CVE-2026-61690
getgrav--grav	Grav is a file-based Web platform. Prior to 2.0.2, the Grav Twig content sandbox permits grav.offsetGet('config') to return the raw configuration object and permits json_encode, print_r, yaml_encode, and string filters to serialize that object without passing through GravSecurityPolicy::checkMethodAllowed. A user with page-author permissions can render sandboxed content that exposes plugins.*	2026-08-19	6.5	CVE-2026-61842

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configuration secrets, including SMTP credentials, API keys, and plugin database credentials. This issue is fixed in version 2.0.2.			
getgrav--grav	Grav before 2.0.15 contains a path traversal vulnerability in the static asset server within index.php that uses string prefix matching instead of directory-boundary validation. Unauthenticated attackers can access files in sibling directories by exploiting directory names that extend the base path string, such as requesting assets-secret when assets is the configured base.	2026-08-18	5.9	CVE-2026-74907
getgrav--grav	Grav Form Plugin before 9.1.19 fails to escape field-definition properties including prepend, append, spacer text, section text, and select option labels in form templates. Attackers with form authoring privileges can inject arbitrary HTML and JavaScript that executes for all form visitors through unescaped raw filters and unquoted attributes.	2026-08-18	5.4	CVE-2026-75107
getgrav--grav	Grav before 2.0.14 contains a stored cross-site scripting vulnerability in the Security::detectXss() function (system/src/Grav/Common/Security.php). All XSS detection patterns use the PCRE /u (UTF-8) modifier, so a single invalid UTF-8 byte anywhere in page content causes preg_match() to return false for every pattern, silently bypassing the save-time XSS safety gate (Validation::checkSafety()). An authenticated attacker with page-edit permissions (without the security.xss_whitelist privilege) can store malicious JavaScript that executes in the browser of a visitor who views the affected page.	2026-08-18	5.4	CVE-2026-75834
getgrav--grav	Grav plugin-api before 1.0.15 contains a script injection vulnerability where the SVG sanitizer only checks for the exact extension 'svg', allowing .svgz and .xhtml files to bypass sanitization and be stored unsanitized. Attackers with api.media.write permission can upload files containing executable script payloads that execute in the site origin when accessed by administrators or visitors.	2026-08-18	4.6	CVE-2026-74908
getgrav--grav	The Grav API plugin (getgrav/grav-plugin-api, bundled with Grav 2.0) before version 1.0.14 (fixed in 1.0.15) contains a missing authorization vulnerability in BlueprintPathResolver::resolveUserScope(). The method gates the users/<name> scope on the account's raw super-admin ACL flag (access.api.super) instead of validating the presented API key's actual scope. An attacker holding an API key scoped only to api.media.write minted on a super-admin account can bypass the authorization check and, via POST /blueprint-upload or GET /blueprint-files, write a file into another user's scope (in the shared user/accounts/ directory, constrained to image extensions by assertSafeExtension()) and browse that scope's file listing, despite the key not being granted api.users.write.	2026-08-18	4.3	CVE-2026-75832
getgrav--grav	The Grav API plugin (getgrav/grav-plugin-api, bundled with Grav 2.0's admin-next/API stack) before version 1.0.14 contains an open redirect weakness in SsoController::sanitizeReturnTo(). The function rejects a literal '/' prefix but does not account for browsers normalizing backslashes to slashes in special (http/https) schemes, so a returnTo value such as '/\evil.com' passes the guard and is later resolved by the browser as the protocol-relative URL '//evil.com'. Following a legitimate OAuth login flow, an attacker-supplied returnTo parameter could redirect an authenticated victim to an attacker-controlled site for post-login phishing. Full browser-side exploitability depends on the admin-next SPA's client-side oauth-callback handler and was not independently verified by the reporter.	2026-08-18	4.2	CVE-2026-75833
getgrav--grav	Grav API plugin (getgrav/grav-plugin-api) before 1.0.14 contains a missing authorization vulnerability in userPassesAuthorize() (AbstractApiController.php). The function fails to consult the calling request's API key scopes, relying instead on the account's raw super-admin flag and ACL grants. As a result, an authenticated attacker holding a scoped API key minted on a privileged account can bypass their declared scope restrictions to access authorize-gated UI metadata and item definitions (sidebar/menubar/widget items and users-list columns/row-actions/filter-tabs) that their key scope should deny, resulting in information disclosure.	2026-08-18	4.3	CVE-2026-75835

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getgrav--grav-plugin-api	Grav API Plugin is a RESTful API for Grav CMS that provides full headless access to your site's content. Prior to 1.0.2, the Grav API plugin POST /api/v1/media pipeline in HandlesMediaUploads::processUploadedFile() validates an SVG filename extension but does not invoke Security::sanitizeSVG(). An attacker with api.media.write permission can store an SVG containing JavaScript, and the server returns the file as Content-Type: image/svg+xml so the script executes when a victim opens it, allowing session data theft and authenticated actions. This issue is fixed in version 1.0.2.	2026-08-19	4.6	CVE-2026-61607
getgrav--grav-plugin-flex-objects	Grav Flex Objects Plugin allows you to build custom collections of objects. Prior to 1.4.3, the Grav Flex Objects Admin Next API requireFlexPermission() method in classes/Api/FlexApiController.php returns without denying access when a directory blueprint omits config.admin.permissions. An authenticated account with only api.access can use the index, show, create, update, delete, export, and media handlers for a permission-less directory even though the core admin.flex-object.authorization fallback would deny the same actions. This issue is fixed in version 1.4.3.	2026-08-19	6.3	CVE-2026-62670
getgrav--grav-plugin-login	Grav Login Plugin adds login, basic ACL, and session wide messages to Grav. Prior to 3.8.11, the Grav Login plugin login.regenerate2FASecret task accepts a top-level GET request through the TaskServiceProvider task: URI parameter without requiring a login-form nonce, an Origin check, or a Referer check. Under the default SameSite=Lax session cookie policy, an off-site navigation can invoke taskRegenerate2FASecret() in a logged-in victim's session, overwrite the victim's TOTP secret, and force two-factor re-enrollment. This issue is fixed in version 3.8.11.	2026-08-19	5.4	CVE-2026-62671
getkin--kin-openapi	kin-openapi is a Go project for handling OpenAPI files. From 0.2.0 until 0.144.0, openapi3filter.ValidateRequest can encounter a NULL-pointer-dereference denial of service when an operation declares a content parameter whose application/json media type has no schema. In openapi3filter/req_resp_decoder.go, the default defaultContentParameterDecoder dereferences mt.Schema.Value without checking whether mt.Schema is nil, even though doc.Validate() accepts the document under OpenAPI 3.0.x and 3.1.x. A single unauthenticated request supplying the parameter value can panic request validation, causing an aborted request with log growth in the common synchronous net/http path or a full process crash in integrations without recovery. This issue is fixed in version 0.144.0.	2026-08-18	5.3	CVE-2026-73502
ggml-org--llama.cpp	A vulnerability was determined in ggml-org llama.cpp bec4772f6. This affects the function rpc_server::graph_compute of the file ggml/src/ggml-rpc/ggml-rpc.cpp of the component ggml-RPC Server. Executing a manipulation can lead to null pointer dereference. The attack may be launched remotely. The pull request to fix this issue awaits acceptance.	2026-08-23	5.3	CVE-2026-78148
gitpython-developers--GitPython	GitPython versions before 3.1.58 fail to validate options passed to git rm and git checkout commands in IndexFile.remove() and Head.checkout(). Attackers can supply --pathspec-from-file and --pathspec-file-nul parameters to read arbitrary files accessible to the process, with full file contents returned in GitCommandError.stderr.	2026-08-19	6.5	CVE-2026-76217
goauthentik--authentik	authentik is an open-source identity provider. Prior to 2026.2.6 and 2026.5.5, a diagnostic action on the LDAP Source API does not enforce the object-level read-authorization filter used by the rest of the API. Any party able to reach the API, including an unauthenticated client, can invoke the diagnostic action against a configured LDAP Source. The server then connects to the upstream directory using the source's configured bind credentials and returns a bounded set of directory entries. The response exposes the distinguished names of those entries and the names of the attributes present on them, revealing directory structure, naming conventions, and the existence of specific accounts and groups, but not attribute	2026-08-18	5.3	CVE-2026-55106

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	values. Deployments without a configured LDAP Source are not affected. This issue is fixed in versions 2026.2.6 and 2026.5.5.			
GreyDGL--PentestGPT	A vulnerability was determined in GreyDGL PentestGPT up to 1.0.0. This vulnerability affects unknown code of the component Web-Page Crawling. Executing a manipulation of the argument Traceback can lead to injection. The attack can be executed remotely. A high complexity level is associated with this attack. It is stated that the exploitability is difficult. The exploit has been publicly disclosed and may be utilized. The reported GitHub issue was closed with the label "not planned".	2026-08-20	5	CVE-2026-76993
gkability--snipe-it	Snipe-IT is an IT asset/license management system. Prior to 8.6.1, a user with the import permission can use CSV update mode to overwrite the email address of a non-admin user and then request a password reset to take over that account. app/Importer/UserImporter.php applies the canEditAuthFields gate by unsetting username, email, password, and activated on the model, but app/Importer/ItemImporter.php sanitizeItemForUpdating() rebuilds the update array from the raw CSV row in \$this->item, restoring the unauthorized values. The app/Http/Controllers/ImportController.php import path checks import permission but does not require users.edit. This issue is fixed in version 8.6.1.	2026-08-19	6.5	CVE-2026-49976
gkability--snipe-it	Snipe-IT is an IT asset/license management system. Prior to 8.4.1, a non-superadmin can use app/Http/Controllers/Assets/BulkAssetsController.php update() to submit company_id directly without Company::getIdForCurrentUser(), allowing assets to be moved across company boundaries and breaking multi-tenant isolation. This issue is fixed in version 8.4.1.	2026-08-19	6.3	CVE-2026-55482
gkability--snipe-it	Snipe-IT is an IT asset/license management system. Prior to 8.6.1, POST /two-factor has no rate limiting, lockout, or attempt counter, allowing an attacker with valid credentials to submit unlimited TOTP guesses against the three accepted codes created by config/google2fa.php window=1. A successful guess creates a fully authenticated session. When two_factor_enabled is 1, POST /account/profile with two_factor_optin=0 can disable two-factor authentication without OTP reverification, while required mode 2 prevents that opt-out. An administrator can also use POST /api/v1/users/two_factor_reset to clear another user's secret. This issue is fixed in version 8.6.1.	2026-08-19	5.9	CVE-2026-49870
gkability--snipe-it	Snipe-IT is an IT asset/license management system. Prior to 8.5.0, a user who can edit other users can reset a superadmin's two-factor authentication through app/Http/Controllers/Api/UsersController.php postTwoFactorReset(). The endpoint authorizes update access but does not enforce canEditAuthFields before clearing two_factor_secret and two_factor_enrolled. This issue is fixed in version 8.5.0.	2026-08-19	5.8	CVE-2026-50550
gkability--snipe-it	Snipe-IT is an IT asset/license management system. Prior to 8.4.1, an authenticated user with generic asset edit permission can delete files attached to assets outside the user's ownership or company assignment. The destroy() methods in app/Http/Controllers/Api/UploadedFilesController.php and app/Http/Controllers/UploadedFilesController.php authorize update against the object class instead of the resolved object instance, creating an insecure direct object reference. This issue is fixed in version 8.4.1.	2026-08-19	5.4	CVE-2026-55519
gkability--snipe-it	Snipe-IT is an IT asset/license management system. Prior to 8.6.3, any activated account can request /maintenances/{id} and read maintenance records for assets in the same company without asset or maintenance permission. app/Http/Controllers/MaintenancesController.php show() renders the record without authorize(), while company-scoped route-model binding only prevents access to other companies. Disclosed fields include asset tags, suppliers, purchase costs, notes, and dates. This issue is fixed in version 8.6.3.	2026-08-19	4.3	CVE-2026-55703

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
h2o--picotls	Picotls is a TLS protocol library that allows users select different crypto backends based on their use case. Picotls implements its own ASN.1 validation helper, which is used by the minicrypto backend while parsing local PKCS#8 private keys. Prior to commit c14231d801407640bc42c2dcf92783409ea6a7c7, the validator recursively descends into constructed ASN.1 elements without enforcing a maximum nesting depth. If an application loads an attacker-supplied private-key file through ptls_minicrypto_load_private_key(), or otherwise calls the public ASN.1 validation API on untrusted DER, a crafted deeply nested ASN.1 structure can exhaust the process stack and crash the application. Note that the libcrypto (OpenSSL) backend does not use the ASN.1 validation helper of picotls, and therefore is immune to this vulnerability. The vulnerability has been addressed in commit c14231d801407640bc42c2dcf92783409ea6a7c7.	2026-08-21	5.5	CVE-2026-45271
Hakan Ozevin--WP BASE Booking	Subscriber Cross Site Scripting (XSS) in WP BASE Booking <= 6.3.2 versions.	2026-08-20	6.5	CVE-2026-73402
hashcat--hashcat	hashcat master branch builds after v7.1.2 contain a heap buffer overflow vulnerability in the KeePass AESKDF/KDBX v4 module (module 34301) that allows attackers to corrupt adjacent heap memory by supplying an oversized ninth hash field token. The module accepts up to 600 hex characters for the ninth token field but decodes it into a fixed 256-byte buffer with no length check, allowing a maximal input to write up to 44 bytes past the buffer boundary into adjacent esalt fields and heap chunk metadata, potentially enabling heap corruption or memory access violations.	2026-08-17	6.1	CVE-2026-68765
hashcat--hashcat	hashcat's fgetl() function in src/filehandling.c writes a null terminator one byte past the caller's buffer when an input line is exactly the buffer length. Attackers can trigger this out-of-bounds heap write by providing a hash file, potfile, or wordlist containing a line of exactly HCBUFSIZ_LARGE bytes.	2026-08-22	6.1	CVE-2026-68767
hashcat--hashcat	hashcat contains a heap-based buffer overflow (out-of-bounds write) in the outfile_write() function in src/outfile.c. When assembling output into a fixed-size buffer (HCBUFSIZ_LARGE, ~16 MB), the function sequentially appends the username, separator, hash, and plaintext via memcpy without validating that the accumulated length stays within the buffer capacity. When run with --username --show against a crafted hash file containing an oversized username that nearly fills the buffer, the total assembled output exceeds the buffer, causing a heap buffer overflow that can corrupt memory and crash the process.	2026-08-22	6.1	CVE-2026-68768
HashiCorp--go-slug	HashiCorp go-slug 0.4.0 through 0.18.2 could allow a local attacker to bypass .terraformignore exclusions and cause sensitive files to be included in Terraform slug uploads due to improper handling of Unicode normalization during path matching.	2026-08-19	5.5	CVE-2026-14978
HCL Software--IEM	HCL IntelliOps Event Management (IEM) is affected by a least privileges violation which could allow an attacker to access the resource with the elevated privilege that could not be accessed with the attacker's original privileges.	2026-08-20	6.6	CVE-2025-62299
HCL Software--IEM	HCL IntelliOps Event Management (IEM) is affected by a race condition. A "timing window" can occur where an attacker can modify the resource causing unpredictable behavior.	2026-08-20	5.9	CVE-2025-62300
HCL Software--IEM	HCL IntelliOps Event Management (IEM) is affected by information omission. The lack of information breaks auditability and observability of a workflow. if an attacker were to gain access to the application, the insufficient logging could hinder incident response.	2026-08-20	5	CVE-2025-62306
HCL Software--IEM	HCL IntelliOps Event Management (IEM) is affected by insufficient logging. Insufficient logging weakens accountability, obscures attack detection, and enables privilege probing.	2026-08-20	5.4	CVE-2025-62307

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
HCL Software--IEM	HCL IntelliOps Event Management (IEM) is affected by missing or insecure Cross-Origin Security headers. This issue makes the application's environment and resources susceptible to unauthorized external interaction and potential exploitation.	2026-08-20	4.8	CVE-2026-21784
Huawei--HarmonyOS	Permission control vulnerability in the Gallery module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-08-17	6.2	CVE-2026-49301
Huawei--HarmonyOS	Permission control vulnerability in the notification service module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-08-17	6.2	CVE-2026-49302
Huawei--HarmonyOS	Permission control vulnerability in the device key management module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-08-17	6.2	CVE-2026-49304
Huawei--HarmonyOS	Permission control vulnerability in the Wi-Fi enhancement module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-08-17	6.2	CVE-2026-49305
Huawei--HarmonyOS	Permission control vulnerability in the multi-mode input module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-08-17	6.2	CVE-2026-49307
Huawei--HarmonyOS	Permission control vulnerability in the notification module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-08-17	5.1	CVE-2026-49303
Huawei--HarmonyOS	Permission control vulnerability in the clipboard module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-08-17	5.5	CVE-2026-49308
Huawei--HarmonyOS	Null pointer dereference issue in the image codec module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-08-17	4	CVE-2026-58560
Huawei--HarmonyOS	Null pointer dereference issue in the image codec module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-08-17	4	CVE-2026-58561
huggingface--transformers	Hugging Face Transformers fails to validate shard filenames in checkpoint index files, allowing attackers to read arbitrary files outside the model directory. Attackers can supply malicious index files with parent-directory references or absolute paths that are joined without validation, enabling file disclosure and filesystem reconnaissance.	2026-08-17	5.5	CVE-2026-75104
iberezansky--3D FlipBook PDF Flipbook Viewer, Flipbook Image Gallery	Unauthenticated Sensitive Data Exposure in 3D FlipBook - PDF Flipbook Viewer, Flipbook Image Gallery <= 1.16.20 versions.	2026-08-18	5.3	CVE-2026-74007
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a null pointer dereference.	2026-08-19	6.5	CVE-2026-16846
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to an out-of-bounds write.	2026-08-19	6.7	CVE-2026-16914
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to execute arbitrary code due to a stack-based buffer overflow.	2026-08-20	6.7	CVE-2026-16944
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local authenticated attacker to execute arbitrary code due to a heap-based buffer overflow.	2026-08-20	6.7	CVE-2026-16951
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an out-of-bounds write.	2026-08-20	6.5	CVE-2026-16958
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to intercept messages and forge replies due to the exposure of sensitive information.	2026-08-20	6.5	CVE-2026-16964

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to obtain sensitive information due to improper authentication.	2026-08-20	6.5	CVE-2026-16972
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service due to improper validation of symbolic links.	2026-08-20	6.3	CVE-2026-16980
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to obtain sensitive information or cause a denial of service due to an out-of-bounds read.	2026-08-20	6.7	CVE-2026-17007
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service due to an out-of-bounds write.	2026-08-20	6.5	CVE-2026-17195
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 A stack memory corruption vulnerability exists in the AIX IPsec ESP decapsulation handler. Successful exploitation may corrupt kernel stack state and cause a system crash, resulting in denial of service.	2026-08-20	6.5	CVE-2026-19448
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service due to improper handling of memory page table configurations.	2026-08-19	6.5	CVE-2026-19653
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause kernel memory corruption due to insufficient validation. A crafted filesystem image can trigger an out-of-bounds kernel-stack write during directory reads, causing a system crash or potentially enabling privilege escalation.	2026-08-20	6.7	CVE-2026-19783
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to the use of an uninitialized stack pointer.	2026-08-19	5.9	CVE-2026-16827
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a NULL pointer dereference.	2026-08-19	5.3	CVE-2026-16829
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to disclose kernel memory due to an out-of-bounds read.	2026-08-19	5.3	CVE-2026-16833
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service due to a heap buffer overflow.	2026-08-19	5.5	CVE-2026-16855
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to obtain sensitive information due to an out-of-bounds read.	2026-08-19	5.5	CVE-2026-16883
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service due to uncontrolled resource consumption.	2026-08-20	5.5	CVE-2026-16952
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to disclose sensitive kernel memory due to an out-of-bounds read.	2026-08-20	5.5	CVE-2026-16973
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a buffer overflow.	2026-08-20	5.3	CVE-2026-17120
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to a stack-based buffer overflow.	2026-08-20	5.4	CVE-2026-18828
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote authenticated attacker to obtain sensitive information and cause a denial of service due to an out-of-bounds write.	2026-08-19	4.2	CVE-2026-16825
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an improper check for an array index boundary.	2026-08-19	4.3	CVE-2026-16849
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an out-of-bounds read.	2026-08-19	4.8	CVE-2026-16866

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to cause a denial of service due to an out-of-bounds write.	2026-08-19	4.3	CVE-2026-16886
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service due to an out-of-bounds write.	2026-08-19	4.4	CVE-2026-16897
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service due to a NULL pointer dereference.	2026-08-20	4.7	CVE-2026-17009
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to bypass security restrictions due to improper limitation of a pathname to a restricted directory.	2026-08-20	4.8	CVE-2026-17424
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to cause a denial of service due to uncontrolled resource consumption when parsing directory records.	2026-08-20	4.4	CVE-2026-18822
IBM--DS8A00 (R10.0 - R10.1)	IBM System Storage DS8A00 10.1.3.0 through 10.11.35.0 and IBM DS8900F 89.40.83.0 through 89.44.25.0 could allow an authenticated user to read or modify another user's command history due to an externally controlled filename.	2026-08-19	5.4	CVE-2025-36398
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to cause a denial of service and obtain sensitive information due to an out-of-bounds read.	2026-08-19	5.4	CVE-2026-17015
IBM--OPENBMC	IBM OpenBMC FW1060.00 through FW1060.80 is affected by a vulnerability in the BMC firmware update process. An attacker with authenticated administrator-level access to the BMC can, under specific conditions, execute arbitrary code, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	6.8	CVE-2026-18849
IBM--Power Systems Firmware	IBM Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in access controls over privileged system configuration operations on the FSP. An attacker with authenticated administrator-level access to the FSP can place the managed system into a non-production operational mode, allowing certain system components to be disabled. This condition persists across FSP resets and requires explicit operator intervention - clearing the affected configuration - to restore normal operation. Successful exploitation results in an availability impact to the managed system.	2026-08-19	6.9	CVE-2026-16938
IBM--Power Systems Firmware	Power Systems Firmware FW1120.00, FW1110.00 through FW1110.30, and FW1060.00 through FW1060.80 is affected by a vulnerability in the host firmware. An attacker with service access to the service processor can supply a carefully crafted command that could leak the contents of hardware registers that should be inaccessible to the service processor. Successful exploitation could result in limited confidentiality or availability impacts to the affected host system.	2026-08-19	6.7	CVE-2026-19321
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in partition firmware during network boot. An unauthenticated attacker with access to the same network as a partition undergoing iSCSI SAN network boot can prevent that partition from completing its boot sequence. Other partitions and the managed system are not affected. Only partitions actively performing an iSCSI SAN network boot are affected, resulting in an availability impact.	2026-08-19	6.5	CVE-2026-17028
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1120.00, FW1110.00 through FW1110.30, and FW1060.00 through FW1060.80 IBM PowerVM could allow a local attacker to obtain sensitive information or cause a denial of service due to improper control of format strings.	2026-08-19	5.2	CVE-2026-15961
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor Platform KeyStore (PKS) and virtual TPM FW1110.00 through FW1110.20, FW1060.00 through FW1060.71, and FW950.00 through FW950.H2 use persistent storage key seeds that result in an AES key with reduced	2026-08-19	5.1	CVE-2026-4936

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	strength. An attacker with access to the service processor or HMC could exploit this weakness to derive the encryption key and access the data.			
IBM--PowerVM Hypervisor	IBM PowerVM Hypervisor FW1110.00 through FW1110.20, FW1060.00 through FW1060.71, and FW950.00 through FW950.H2 could allow a local attacker with administrative privileges to decrypt encrypted data due to certain hypervisor calls utilizing less entropy than requested.	2026-08-19	5.3	CVE-2026-4937
IBM--Reliable Scalable Cluster Technology (RSCT)	IBM Reliable Scalable Cluster Technology (RSCT) 3.0 could allow a remote attacker to cause a denial of service by sending a specially crafted request due to improper input validation.	2026-08-19	6.5	CVE-2026-14514
IBM--Server Firmware	IBM Server Firmware FW1120.00, FW1110.00 through FW1110.30, FW1060.00 through FW1060.80, and FW950.00 through FW950.H2 is affected by a vulnerability in the FSP firmware update process. An attacker with authenticated administrator-level access to the FSP can, under specific conditions, execute arbitrary code, resulting in a confidentiality, integrity, and availability impact.	2026-08-19	6.8	CVE-2026-18681
IBM--Virtualization Management Interface	IBM Virtualization Management Interface FW1110.00 through FW1110.30, FW1120.00 through FW1120.00, and FW1060.00 through FW1060.80 is affected by a vulnerability in the Virtualization Management Interface (VMI). An attacker with authenticated administrator-level access can cause the VMI to crash. The VMI will restart automatically; however, repeated exploitation could result in a sustained availability impact.	2026-08-19	4.5	CVE-2026-16724
IKAS Technology Inc.--Rush	Missing authentication for critical function vulnerability in IKAS Technology Inc. Rush allows Fake the Source of Data. This issue affects Rush: through 21082026.	2026-08-21	5.3	CVE-2026-19441
Insyde Software--InsydeH2O, InsydeH2O ARM	On ARM platforms, a vulnerability in the architecture design of HDD Password could allow an attacker to retrieve HDD Password from UEFI variables.	2026-08-19	6.9	CVE-2026-8810
InternationalColor Consortium--iccDEV	iccDEV provides a set of libraries and tools for working with ICC color management profiles. Versions prior to 2.3.2.1 have a `ClccEmbedIO::Read8()` size_t underflow. The issue arises due to an embedded-profile read defect when parsing ICC profiles containing `icSigEmbeddedV5ProfileTag` data with `icSigEmbeddedProfileType` payloads. Version 2.3.2.1 patches the issue. No known workarounds are available.	2026-08-21	6.5	CVE-2026-50278
itsourcecode--Hospital Management System	A vulnerability has been found in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /viewpatient.php. Such manipulation of the argument delid leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2026-08-17	6.3	CVE-2026-19972
itsourcecode--Hospital Management System	A vulnerability was found in itsourcecode Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /viewpaymentreport.php. Performing a manipulation of the argument delid results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	2026-08-17	6.3	CVE-2026-19973
itsourcecode--Hospital Management System	A vulnerability was detected in itsourcecode Hospital Management System 1.0. The impacted element is an unknown function of the file /viewprescriptionrecord.php. The manipulation of the argument delid results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	2026-08-17	6.3	CVE-2026-20000
itsourcecode--Hospital Management System	A vulnerability has been found in itsourcecode Hospital Management System 1.0. The impacted element is an unknown function of the file /viewroom.php. Such manipulation of the argument delid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2026-08-18	6.3	CVE-2026-75086
itsourcecode--Hospital	A vulnerability was found in itsourcecode Hospital Management System 1.0. This affects an unknown function of the file /viewdepartment.php. Performing a	2026-08-18	6.3	CVE-2026-75087

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	manipulation of the argument delid results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.			
itsourcecode--Hospital Management System	A vulnerability was determined in itsourcecode Hospital Management System 1.0. This impacts an unknown function of the file /viewbilling.php. Executing a manipulation of the argument delid can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-18	6.3	CVE-2026-75088
itsourcecode--Hospital Management System	A vulnerability was found in itsourcecode Hospital Management System 1.0. This affects an unknown part of the file /viewappointmentapproved.php. Performing a manipulation of the argument delid results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2026-08-20	6.3	CVE-2026-76991
itsourcecode--Hospital Management System	A weakness has been identified in itsourcecode Hospital Management System 1.0. This affects an unknown part of the file /viewappointmentpending.php. This manipulation of the argument delid causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-20	6.3	CVE-2026-77025
itsourcecode--Hospital Management System Project in PHP	A flaw has been found in itsourcecode Hospital Management System Project in PHP 1.0. This impacts an unknown function of the file /viewservicetype.php. This manipulation of the argument delid causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2026-08-23	6.3	CVE-2026-78112
jae-jae--fetcher-mcp	A vulnerability has been found in jae-jae fetcher-mcp up to 0.3.9. Impacted is the function fetch_url/fetch_urls of the file /latest/meta-data/iam/security-credentials/ of the component URL Validation. Such manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-17	6.3	CVE-2026-74858
jahives--openssl_encrypt	openssl_encrypt versions before 1.4.6 contain a key derivation flaw in sequential XOR composition mode where the last stage cancels out during key generation. When configured with a single KDF and no prior hashing stage, attackers can bypass memory-hard key derivation and perform offline password cracking at SHA-256 speed instead of the configured KDF cost.	2026-08-17	6.2	CVE-2026-74871
jahives--openssl_encrypt	openssl_encrypt versions before 1.4.0 configure CORS with allow_origins set to wildcard and allow_credentials enabled to true. Attackers can create malicious websites that make authenticated cross-origin requests to the API on behalf of any user who visits them.	2026-08-17	6.5	CVE-2026-74881
jahives--openssl_encrypt	openssl_encrypt versions before 1.4.0 expose passwords passed via the --password CLI argument in process listings accessible to all system users. Attackers can read process arguments through ps aux or /proc/[pid]/cmdline to retrieve plaintext passwords and keystore passwords.	2026-08-17	5.5	CVE-2026-74873
jahives--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain an authentication bypass vulnerability in CamelliaCipher that disables HMAC tag generation and verification when the PYTEST_CURRENT_TEST environment variable is set. Attackers with code execution can set this environment variable to produce unauthenticated ciphertext and bypass integrity protection on encrypted data.	2026-08-17	5.5	CVE-2026-74890
jdx--mise	mise manages dev tools like node, python, cmake, and terraform. Prior to 2026.7.1, release tar archives record mise/bin/mise with user and group ID 1001 and packaging/standalone/install.envsubst extracts and moves it without normalizing ownership, allowing a local user with those IDs to replace a root-installed executable, especially when MISE_INSTALL_PATH targets a shared location such as /usr/local/bin. This issue is fixed in version 2026.7.1.	2026-08-18	6.7	CVE-2026-71477
JetBrains--IntelliJ IDEA	In JetBrains IntelliJ IDEA before 2026.2.1 sSRF was possible via the OpenAPI preview proxy in untrusted projects	2026-08-17	6.3	CVE-2026-75054

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
JetBrains--IntelliJ IDEA	In JetBrains IntelliJ IDEA before 2026.1.5 git credentials were written in plaintext to the IDE log	2026-08-17	6.2	CVE-2026-75057
JetBrains--IntelliJ IDEA	In JetBrains IntelliJ IDEA before 2026.2.1 sSRF was possible via the DevKit debug listener endpoint	2026-08-17	5.4	CVE-2026-75053
JetBrains--IntelliJ IDEA	In JetBrains IntelliJ IDEA before 2026.2.1 hadoop ResourceManager could read local files via XXE	2026-08-17	5.5	CVE-2026-75055
JetBrains--IntelliJ IDEA	In JetBrains IntelliJ IDEA before 2026.2.1 xXE was possible in the Eclipse settings importers	2026-08-17	5.5	CVE-2026-75058
JetBrains--Ktor	In JetBrains Ktor before 3.4.1 potential DoS attack via WebSocket decompression was possible	2026-08-17	5.9	CVE-2026-68762
JetBrains--PyCharm	In JetBrains PyCharm before 2026.2.1 code execution via Quick Documentation was possible	2026-08-17	4.4	CVE-2026-75059
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.18177 doS attack was possible via a decompression bomb in the import endpoint	2026-08-17	6.5	CVE-2026-75047
JetBrains--YouTrack	In JetBrains YouTrack before 2026.1.13903, 2026.2.17950 an authenticated user could read restricted articles from other projects via the draft creation endpoint	2026-08-17	6.5	CVE-2026-75049
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.18112 an authenticated user could enumerate accounts via the users search endpoint	2026-08-17	4.3	CVE-2026-75046
jiantao88--android-mcp-server	A flaw has been found in jiantao88 android-mcp-server up to cfb872b2446794193b58edd63f4dbf6af48a6292. The impacted element is the function child_process.exec of the file build/index.js of the component Command Execution. Executing a manipulation of the argument deviceId/packageName/permission/extras[].key/extras[].value can lead to os command injection. It is possible to launch the attack on the local host. The exploit has been published and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. This patch is called 14e2bf27c88ba137e35cbb0c2a75f72b595bb98a. It is advisable to implement a patch to correct this issue.	2026-08-17	5.3	CVE-2026-19978
jkawamoto--mcp-florence2	A flaw has been found in jkawamoto mcp-florence2 up to 0.3.13. Affected by this issue is the function get_images of the file src/mcp_florence2/__init__.py. This manipulation of the argument src causes server-side request forgery. The attack may be initiated remotely. The exploit has been published and may be used. It is recommended to change the configuration settings. The vendor explains: "For deployments where SSRF protection is required, I recommend routing all HTTP(S) requests through an SSRF-safe proxy server. This approach mitigates the vulnerability without requiring changes to the mcp-florence2 source code."	2026-08-17	6.3	CVE-2026-19984
jkulmann--cgltf	cgltf through 1.15 contains an integer overflow vulnerability in the non-sparse accessor bounds check within cgltf_validate() that allows remote attackers to cause memory disclosure and denial of service by supplying crafted accessor count values. Attackers can provide malformed .gltf or .glb input with a specially crafted accessor count to overflow the unsigned integer multiplication of accessor stride and element count, causing the bounds check to pass and triggering a heap out-of-bounds read when cgltf_accessor_read_float() is subsequently called on the validated malformed accessor.	2026-08-19	6.1	CVE-2026-75148
juicedata--juicefs	The filestore backend in pkg/object/file.go, used for file:// stores and as a common juicefs sync destination, derived every operation's target from path(key), which returned either filepath.Join(d.root, key) or filepath.Clean(d.root + key) with no check that the result stayed beneath the root. Put, Get, Head, Delete, Chmod, Chown, Symlink and Readlink all consumed that value directly. Object keys enumerated from a source object store during a sync are not constrained the way	2026-08-21	6.5	CVE-2026-77763

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	local filesystem names are, so a key containing traversal segments causes juicefs to write attacker-supplied content to a path outside the intended local destination, and no error is returned. An operator syncing from a bucket whose contents they do not fully control, such as a shared or public bucket or one an attacker can write to, is therefore exposed to a file write at an attacker-influenced location. The fix changes path() to return an error and rejects any key whose resolved path escapes the root.			
jumpserver--jumpserver	JumpServer is an open source bastion host and an operation and maintenance security audit system. Prior to 4.10.17, an authenticated administrator with Applet Host management and deployment permissions can inject Jinja2 expressions into the IP/Host field or Core Service Address field, causing Ansible to evaluate ansible_host inventory data or playbook variables during Applet Host deployment and execute arbitrary commands on the JumpServer control node. This issue is fixed in version 4.10.17.	2026-08-17	6.7	CVE-2026-44845
jumpserver--jumpserver	JumpServer is an open source bastion host and an operation and maintenance security audit system. Prior to 4.10.17, a user with the users.invite_user permission can submit an existing member to POST /api/v1/users/users/invite/, causing the organization invitation logic in apps/users/api/user.py to execute user.org_roles.set(org_roles) and replace the member's existing organization roles, which can escalate privileges or downgrade administrators. This issue is fixed in version 4.10.17.	2026-08-17	6.2	CVE-2026-44846
jumpserver--jumpserver	JumpServer is an open source bastion host and an operation and maintenance security audit system. From 4.8.0 until 4.10.17, an authenticated user with SFTP permission to an authorized asset can submit crafted traversal paths through the KoKo Web Terminal SFTP feature, causing AssetDir.GetRealPath() in pkg/srvconn/sftp_asset.go to resolve paths outside the intended SFTP root and permit read, list, write, rename, or delete operations under the configured backend account on that asset. This issue is fixed in version 4.10.17.	2026-08-17	5.4	CVE-2026-54336
kedacore--keda	KEDA is a Kubernetes-based Event Driven Autoscaling component. Prior to 2.20.0, pkg/scalers/postgresql_scaler.go constructs libpq-style connection strings from tenant-controlled host, port, userName, dbName, sslmode, and password values, while escapePostgreConnectionParameter() only quotes values containing a literal space. Tabs, newlines, carriage returns, form feeds, vertical tabs, quotes, and backslashes can therefore create additional key-value tokens when pgx parses the string. An attacker able to create or modify a TriggerAuthentication or ScaledObject can inject host or sslmode parameters, redirect the database connection to an attacker-controlled server, expose credentials, or disable intended TLS protection. This issue is fixed in version 2.20.0.	2026-08-21	5.9	CVE-2026-53572
Kings Plugins--B2BKing	Missing Authorization vulnerability in Kings Plugins B2BKing allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects B2BKing: from n/a through 5.2.30.	2026-08-18	5.4	CVE-2026-66589
Kira-Pgr--PromptShopMCP	A vulnerability was found in Kira-Pgr PromptShopMCP up to 5bc0cd17358e19a5415d11a531088170d7b81452. Affected is the function download_image of the file server.py of the component Image-Toolkit-MCP-Server. Performing a manipulation of the argument image_url results in server-side request forgery. The attack may be initiated remotely. The exploit has been made public and could be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-17	6.3	CVE-2026-74842
kite-org--kite	Kite is a Kubernetes dashboard. Prior to version 0.12.3, authenticated Kite users with any role can request `/api/v1/overview` for a cluster that their roles do not permit by selecting that cluster with `x-cluster-name`. The overview route is registered before `middleware.RBACMiddleware()` and `GetOverview` only checks	2026-08-21	4.3	CVE-2026-53487

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`len(user.Roles) > 0`, so it returns aggregate Kubernetes inventory and capacity data from unauthorized clusters. Version 0.12.3 fixes the issue.			
KNMI--adaguc-server	Adaguc-server is an open source geographical information system to visualize, combine, compare and share real-time meteorological, climatological and remote sensing data via OGC standards. Versions prior to 7.2.2 crash with a memory-safety fault when it parses a GeoJSON document whose geometry contains a malformed coordinate. The coordinate parser in `adagucserverEC/CConvertGeoJSON.cpp` indexes `pt.u.array.values[0]` and `pt.u.array.values[1]` and uses `polygon.u.array.length` as a loop bound without first validating the JSON node type or the coordinate length. A coordinate that is an empty array, a one-element array, a scalar, or `null` leads to an out-of-bounds heap read or a NULL pointer dereference. The same unchecked pattern is present in four geometry branches: `Polygon`, `LineString`, `MultiLineString` and `MultiPolygon`. The vulnerable parser runs whenever the server processes a local GeoJSON file, either a configured GeoJSON dataset or a GeoJSON file exposed through the `AutoResource` feature and requested by an unauthenticated WMS request. A crafted GeoJSON file reliably crashes the backend process that handles that request. Version 7.2.2 patches the vulnerability.	2026-08-18	4	CVE-2026-50126
koel--koel	Koel is a free, open-source music streaming solution. Prior to 9.7.0, the Subsonic-compatible createPodcastChannel.view route accepts an authenticated user's private URL because app/Http/Requests/Subsonic/CreatePodcastChannelRequest.php does not apply the SafeUrl validation used by the regular podcast API. app/Http/Controllers/Subsonic/CreatePodcastChannelController.php passes the URL to app/Services/Podcast/PodcastService.php, where PodcastService::addPodcast() and createParser() invoke Poddle::fromUrl() during channel creation, causing immediate server-side requests to loopback, Docker bridge, or RFC1918 HTTP destinations. The confirmed impact is blind internal request execution because generic response-body exfiltration was not demonstrated through this route. This issue is fixed in version 9.7.0.	2026-08-19	4.3	CVE-2026-54492
Koha Community--Koha	Koha before 26.05.02, 25.11.07, and 25.05.13 contains a stored cross-site scripting vulnerability in the purchase suggestion handler that allows authenticated staff users to inject malicious scripts by submitting unsanitized input through the suggestion save operation. Attackers can supply crafted HTML or script content in fields such as title, author, isbn, publishercode, place, collectiontitle, itemtype, and note, which are stored without sanitization and later rendered in the suggestion list template, causing injected scripts to execute in the browser of any staff user who views the suggestions.	2026-08-18	5.4	CVE-2026-41921
Kozea--WeasyPrint	WeasyPrint helps web developers to create PDF documents. Prior to 69.0, WeasyPrint embeds unescaped HTML presentational-hint attribute values into CSS in weasyprint/css/_init_.py when presentational_hints=True. The background attribute is inserted into a background-image:url() declaration and parsed by tinycss2.parse_blocks_contents(), allowing untrusted HTML to inject additional CSS declarations. Applications that render untrusted HTML with presentational hints enabled can be affected by CSS injection and server-side requests through injected url() values. This issue is fixed in version 69.0.	2026-08-18	6.5	CVE-2026-49452
Kriptok Crypto and Information Technologies Industry Trade Inc.--Cryptosim	Cleartext storage of sensitive information vulnerability in Kriptok Crypto and Information Technologies Industry Trade Inc. Cryptosim allows Retrieve Embedded Sensitive Data. This issue affects Cryptosim: before 3.1.0.229.	2026-08-18	5.7	CVE-2026-5224
kylecui--NetForensicMCP	A flaw has been found in kylecui NetForensicMCP 2.1.0. Impacted is the function execAsync of the file index.js. Executing a manipulation of the argument interface/protocol can lead to command injection. The attack may be launched	2026-08-17	6.3	CVE-2026-75011

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.			
LabRedesCefetRJ--WeGIA	WeGIA before 3.9.2 contains an insecure direct object reference vulnerability in the employee profile page that allows authenticated attackers to access arbitrary employee records by injecting an id_pessoa parameter through a request extraction function that overwrites the session-derived identifier. Attackers can enumerate all user identifiers to retrieve full profile data for any employee account, including name, CPF, address, contact details, and administrative flags.	2026-08-20	6.5	CVE-2026-76634
LB-Link--WR1210M	A flaw has been found in LB-Link WR1210M 1.0.3. This impacts the function main of the file /www/cgi-bin/backup.cgi of the component Backup Endpoint. This manipulation causes missing authentication. The attack is only possible within the local network. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-17	4.7	CVE-2026-19971
leanprover--lean4	The Lean 4 kernel does not verify that the structure named in a projection expression matches the type of the value being projected, and environment::add_inductive in src/kernel/inductive.cpp did not type check the nested inductive applications that are replaced by auxiliary types, so their parametric arguments escaped checking. A metaprogram running in the Lean process can register an ill-typed nested inductive whose constructor applies a .proj C 0 projection to a value of the unrelated type W, and the kernel admits the declaration through the ordinary checked addDecl path at maximum kernel checking, without sorry, unsafeCast, debug.skipKernelTC, addDeclWithoutChecking, FFI, or a modified .olean file. The result is a type confusion yielding a proof of False that carries no axioms, from which any proposition can be derived. The published proof of concept additionally pads two expressions until their hashes and approximate depths collide, which defeats kernel caching; that is the technique used to reach the flaw, not its cause. Exploitation requires running a metaprogram in-process, for example by building a project or importing a malicious Lake dependency.	2026-08-20	6.3	CVE-2026-72844
learningequality--kolibri	Kolibri is an offline-first education platform. Prior to version 0.19.4, several Kolibri API endpoints accept an unvalidated `baseurl` parameter and fetch attacker-controlled URLs from the Kolibri server, reflecting the response body back to the caller. The original report identified two endpoints on the `RemoteFacilityUser` viewsets; remediation review found two further reflection points on the same pattern. The GET endpoint was unauthenticated. Version 0.19.4 fixes the vulnerability.	2026-08-17	5.8	CVE-2026-48053
LemmyNet--lemmy	Lemmy is a link aggregator and forum for the fediverse. Prior to 0.19.19 and 1.0.0-beta.1, actix-web ConnectionInfo::realip_remote_addr reads the first value of X-Forwarded-For as the client address used by raw_ip_key in crates/utlis/src/rate_limit/mod.rs. Lemmy's bundled docker/nginx.conf uses \$proxy_add_x_forwarded_for instead of \$remote_addr, which appends the real client address to an X-Forwarded-For value supplied by the client. An unauthenticated attacker can therefore place a different spoofed address first on each request and receive a new rate-limit bucket, bypassing limits on POST /api/v4/account/auth/register, POST /api/v4/account/auth/login, POST /api/v4/post, POST /api/v4/comment, GET /api/v4/search, POST /api/v4/image, and POST /api/v4/account/import_settings. This permits excessive account creation, brute-force attempts, spam, scraping, uploads, and repeated imports. This issue is fixed in versions 0.19.19 and 1.0.0-beta.1.	2026-08-19	6.5	CVE-2026-54738
LemmyNet--lemmy	Lemmy is a link aggregator and forum for the fediverse. Prior to 0.19.19 and 1.0.0-alpha.18, a lower-ranked remote moderator can remove a higher-ranked moderator by sending a signed ActivityPub Remove activity to the target instance. The local API uses LocalUser::is_higher_mod_or_admin_check to enforce moderator rank, but CollectionRemove::verify in crates/apub/activities/src/community/collection_remove.rs only calls	2026-08-19	6.5	CVE-2026-54740

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	verify_mod_action. CollectionRemove::receive dereferences self.object as an ApubPerson, creates a CommunityModeratorForm, and calls CommunityActions::leave without checking that the actor outranks the moderator identified by the object field. In communities with federated moderators, a junior moderator can therefore strip senior moderators from the community moderator list even though the local API rejects the same action. This issue is fixed in versions 0.19.19 and 1.0.0-alpha.18.			
libexpat project--libexpat	In libexpat 2.8.2 and 2.8.3 before 2.8.4, misinterpretation of getentropy's return code leads to insufficient entropy, which results in being vulnerable to hash flooding attacks, causing a denial of service via crafted XML content.	2026-08-20	5.9	CVE-2026-76956
libexpat project--libexpat	libexpat before 2.8.4 lacks handler call depth tracking with custom encoding callbacks. Thus, a use-after-free can occur. NOTE: this is similar to CVE-2026-50219, CVE-2026-56131 and CVE-2026-56412.	2026-08-20	4.9	CVE-2026-76957
libgit2--libgit2	libgit2 is a portable C implementation of the Git core methods provided as a linkable library with a solid API, allowing to build Git functionality into your application. Prior to 1.8.6 and 1.9.5, verify_server_cert in src/libgit2/streams/openssl.c uses an inverted !!memcmp result in the GEN_IPADD branch when comparing an IP-literal host with a certificate IP SubjectAltName. OpenSSL builds reject matching IP addresses and accept mismatched IP addresses, allowing a network attacker with a CA-trusted certificate containing any IP SubjectAltName to intercept libgit2 connections to IP-literal HTTPS URLs. DNS SubjectAltName validation and non-OpenSSL TLS backends are not affected. This issue is fixed in versions 1.8.6 and 1.9.5.	2026-08-20	6.5	CVE-2026-53583
libgit2--libgit2	libgit2 is a portable C implementation of the Git core methods provided as a linkable library with a solid API, allowing to build Git functionality into your application. Prior to 1.8.6 and 1.9.5, the built-in HTTP transport in src/libgit2/transport/http.c follows an offsite initial redirect, and handle_remote_auth and handle_auth pass transport->owner->url instead of transport->server.url to the credential callback when the redirected host returns 401 Unauthorized. A callback that scopes credentials to the original trusted URL can therefore return GIT_CREDENTIAL_USERPASS_PLAINTEXT credentials that libgit2 stores in transport->server.cred and sends as an Authorization header to the redirected host. An attacker who controls a trusted Git host or an open redirect on that host can disclose HTTP Basic credentials, personal access tokens, or equivalent credentials. This issue is fixed in versions 1.8.6 and 1.9.5.	2026-08-20	6.5	CVE-2026-53586
libgit2--libgit2	libgit2 is a portable C implementation of the Git core methods provided as a linkable library with a solid API, allowing to build Git functionality into your application. Prior to 1.8.6 and 1.9.5, git_delta_apply in src/libgit2/delta.c trusts the attacker-controlled res_sz value parsed by hdr_sz from a delta object header and passes that amount to git__malloc before validating delta instructions. Malicious pack data supplied through git_clone, git_fetch, git_remote_fetch, git_indexer_append, or a local attacker-supplied repository can use a very small multi-level OFS_DELTA chain to retain extremely large allocations and exhaust memory. This issue is fixed in versions 1.8.6 and 1.9.5.	2026-08-20	5.3	CVE-2026-53585
libgit2--libgit2	libgit2 is a portable C implementation of the Git core methods provided as a linkable library with a solid API, allowing to build Git functionality into your application. Prior to 1.8.6 and 1.9.5, libgit2 does not reject traversal components in a submodule path loaded from .gitmodules. The affected src/libgit2/submodule.c paths include git_submodule_lookup and git_submodule_add_setup. A crafted repository can specify a path such as ../escape-target, and applications that initialize the submodule can create directories outside the repository working tree. This issue is fixed in versions 1.8.6 and 1.9.5.	2026-08-20	4.3	CVE-2026-53584
lifthoff-sr--CIPster	A weakness has been identified in liftoff-sr CIPster 1802525be27d33e19a9a83c163e331a1d13b1892. This affects the function	2026-08-20	5.3	CVE-2026-76988

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CipConnMgrClass::forward_open of the file cipconnectionmanager.cc of the component ForwardOpen Handler. Executing a manipulation of the argument product_code_ can lead to out-of-bounds read. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. This patch is called ea870a274bf68dfaa3f511f20e2fff6778fb7b74. A patch should be applied to remediate this issue.			
liftoff-sr--CIPster	A security vulnerability has been detected in liftoff-sr CIPster 1802525be27d33e19a9a83c163e331a1d13b1892. This impacts an unknown function of the file source/src/enet_encap/encap.cc of the component TCP Encapsulation Receive Path. The manipulation leads to out-of-bounds read. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The identifier of the patch is e8e9dba09bf56962807d3504b783ccdb6287f3e4. To fix this issue, it is recommended to deploy a patch.	2026-08-20	5.3	CVE-2026-76989
lightdash--lightdash	Lightdash stores the webhook URL supplied with a scheduled delivery and later posts to it from sendWebhook in packages/backend/src/clients/GoogleChat/GoogleChatClient.ts and in packages/backend/src/clients/MicrosoftTeams/MicrosoftTeamsClient.ts. In affected versions both call fetch on the stored URL directly. The validatePublicHttpUrl helper in packages/backend/src/utis/ssrfProtection.ts, used for MCP server URLs, is not applied on either path, and the webhook fields carry no server-side URL constraint. A user able to create or trigger a scheduled delivery can therefore direct the server to issue POST requests to private, loopback and link-local addresses, including cloud metadata endpoints, and can distinguish reachable internal services from unreachable ones through the resulting errors. The upstream response is never returned to the requester; on a failure status its body is written to the server log instead. Version 1.146.4 routes both clients through postSchedulerWebhook from packages/backend/src/utis/schedulerWebhookValidation rather than calling fetch directly.	2026-08-20	6.4	CVE-2026-72846
Linuxfabrik--monitoring-plugins	Linuxfabrik Monitoring Plugins provides monitoring plugins for Icinga, Nagios, and related systems. Prior to version 7.0.0, check-plugins/logfile/logfile accepted a free-form --filename path and opened it as root when invoked through the shipped nagios or icinga sudoers allowlist, without confining the resolved path to /var/log. An attacker who controls the monitoring account can select a root-readable file such as /etc/shadow and use --warning-regex . while leaving SUPPRESS_OUTPUT false, causing each nonempty line to be collected in warn_matches and returned through lib.base.oao(). The vulnerable flow passes the expanded scan_path directly to open(), and neither real-path containment nor an allowlist protects the sink. The same fix also confines mysql-logfile and openvpn-client-list paths, allows only documented log roots, and resolves symlinks and parent-directory traversal before checking containment. This issue is fixed in version 7.0.0.	2026-08-18	5.5	CVE-2026-73973
Linuxfabrik--monitoring-plugins	linuxfabrik-lib provides Python modules for database access, caching, shell execution, and API integrations, and Linuxfabrik Monitoring Plugins uses its shared testing helper across check plugins. Prior to linuxfabrik-lib 6.1.0 and Linuxfabrik Monitoring Plugins 7.0.0, lib.lftest.test() treated the first or second element of a --test CSV argument as a filesystem path and returned the file contents as simulated standard output or standard error without path confinement. The hidden but production-accessible --test argument was accepted by sudo-authorized plugins, so an attacker controlling the nagios or icinga account could use check-plugins/deb-updates/deb-updates with its default QUERY=1 to disclose every line of a root-readable file. Approximately 22 other plugins exposed filtered content or a root file existence and readability oracle through the same helper, while check-plugins/network-bonding/network-bonding and check-plugins/openstack-swift-stat/openstack-swift-stat had direct read paths that bypassed the helper. The library fix confines fixture reads to the invoking plugin's unit-test directory and	2026-08-18	5.5	CVE-2026-73974

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	refuses unsafe anchors, and the plugin fix routes the two bypasses through that helper. These issues are fixed in linuxfabrik-lib 6.1.0 and Linuxfabrik Monitoring Plugins 7.0.0.			
LitExtension-- LitExtension	The LitExtension WordPress plugin through 1.2.5 does not verify a nonce before an administrative action that overwrites the store-migration connector's authentication token, allowing attackers to take over the connector token by tricking a logged-in administrator into clicking a crafted link (CSRF).	2026-08-21	4.2	CVE-2026-15046
logto-io--logto	Logto is the modern, open-source auth infrastructure for SaaS and AI apps. From 1.40.1 until 1.41.0, Logto's .github/workflows/commitlint.yml directly interpolated github.event.pull_request.title into the Commitlint on PR title step's inline echo command before piping the title to npx commitlint. A pull request title containing a single quote could terminate the echo string and append arbitrary shell commands on the GitHub Actions runner. The pull_request trigger used a read-only GITHUB_TOKEN and did not expose repository secrets, but injected commands could alter or disrupt the ephemeral workflow execution. This issue is fixed in version 1.41.0.	2026-08-19	6.3	CVE-2026-63187
lxc--incus	Incus is a system container and virtual machine manager. Prior to version 7.3.0, project-level enforcement of `restricted.containers.privilege=isolated` can be trivially bypassed, allowing a user to create a non-isolated (shared host idmap) container in a project that is configured to forbid them. The restriction only rejects an explicitly set `security.idmap.isolated=false` (or empty) and fails to enforce anything when the key is omitted entirely. Because an unset `security.idmap.isolated` defaults to `false` (non-isolation), a user simply leaves the key out and obtains exactly the container state the restriction is meant to forbid. This defeats the tenant-isolation guarantee the restriction exists to provide. Containers in the project share the host uid/gid map instead of receiving unique, non-overlapping ranges, weakening the isolation boundary between co-tenant containers and the host. Version 7.3.0 patches the issue.	2026-08-21	4.3	CVE-2026-62313
magepeopleteam-- Taxi Booking Manager for WooCommerce	Unauthenticated Broken Access Control in Taxi Booking Manager for WooCommerce < 2.0.8 versions.	2026-08-19	6.5	CVE-2026-73363
MagicMirrorOrg-- MagicMirror	MagicMirror ^{Â²} is an open source modular smart mirror platform. Prior to 2.37.0, when hideConfigSecrets is enabled, the catch-all socket dispatcher in js/node_helper.js passes every inbound object payload through replaceSecretPlaceholder in js/server_functions.js before invoking socketNotificationReceived. A client connected to a loaded module namespace can submit a SECRET_API_KEY placeholder, causing the server to replace it with the corresponding process environment value. The default weather helper accepts INIT_WEATHER, copies the attacker-controlled instanceId, and returns it in WEATHER_ERROR, providing an echo path for the expanded secret. This reverses the intended one-way redaction boundary and can disclose API tokens, credentials, or service keys stored in SECRET_ variables. This issue is fixed in version 2.37.0.	2026-08-18	4.3	CVE-2026-63640
Marcin--Wise Chat	Contributor Cross Site Scripting (XSS) in Wise Chat <= 3.4 versions.	2026-08-18	6.5	CVE-2026-66636
Marcus (aka @msykes)--Login With Ajax	Contributor Cross Site Scripting (XSS) in Login With Ajax <= 4.5.1 versions.	2026-08-18	6.5	CVE-2026-66640
Mattermost-- Mattermost	Mattermost versions 11.7.x <= 11.7.6, 10.11.x <= 10.11.21, 11.8.x <= 11.8.3 fails to validate WebSocket command field types which allows an authenticated user to crash the plugin process and deny service to all Boards users via a custom_focalboard_SUBSCRIBE_TEAM message with a non-string teamId.. Mattermost Advisory ID: MMSA-2026-00687	2026-08-17	6.5	CVE-2026-10080

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.6, 10.11.x <= 10.11.21, 11.8.x <= 11.8.3 fails to reconcile SchemeAdmin flags with a user's current role which allows a user demoted to System Guest to retain Board Admin privileges and perform admin-only operations via the Boards REST API or UI.. Mattermost Advisory ID: MMSA-2026-00691	2026-08-17	6.3	CVE-2026-10527
Mattermost--Mattermost	Mattermost versions 11.8.x <= 11.8.2, 11.7.x <= 11.7.6, 10.11.x <= 10.11.21 fail to restrict channel member role assignment to channel-scoped roles which allows a channel administrator to gain additional channel permissions via the channel member roles API.. Mattermost Advisory ID: MMSA-2026-00697	2026-08-17	6.3	CVE-2026-16048
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.6, 10.11.x <= 10.11.21, 11.8.x <= 11.8.3 fail to enforce PermissionManageBoardRoles on the channelId field of the batch endpoint, which allows an authenticated board editor to relink any board they can edit to an arbitrary channel via a crafted PATCH request. Mattermost Advisory ID: MMSA-2026-00686	2026-08-17	6.5	CVE-2026-9859
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.6, 11.8.x <= 11.8.3 The access control policy unassign endpoint fails to re-validate that each target channel still belongs to the requesting admin's team, which allows an authenticated team administrator to remove ABAC (attribute-based access control) policy assignments from channels outside their team via the policy unassign API after a channel has been moved to another team.. Mattermost Advisory ID: MMSA-2026-00718	2026-08-17	4.2	CVE-2026-15754
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.6, 10.11.x <= 10.11.21, 11.8.x <= 11.8.3 fail to validate that users have read access to a channel before linking a board to it, which allows an authenticated attacker to discover the membership of private channels on the same team via creating, patching, importing, or bulk-creating boards with an arbitrary channelId. Mattermost Advisory ID: MMSA-2026-00674	2026-08-17	4.3	CVE-2026-16047
mauriceboe--TREK	TREK is a collaborative travel planner. From 3.0.0 until 3.1.0, the GET /api/journeys/:id/share-link route in server/src/routes/journey.ts returns the result of getJourneyShareLink() from server/src/services/journeyShareService.ts without checking whether the authenticated requester can access the journey. Any ordinary authenticated user can enumerate sequential journey IDs and retrieve tokens from journey_share_tokens for another user's journey. The token grants unauthenticated access through GET /api/public/journey/:token to the shared journey's entries, captions, locations, moods, gallery photos, photo paths, and asset identifiers. This issue is fixed in version 3.1.0.	2026-08-20	6.5	CVE-2026-54509
mauriceboe--TREK	TREK is a collaborative travel planner. Prior to 3.1.3, TREK file upload, update, and link actions accept attacker-controlled reservation_id, place_id, and assignment_id values without using findForeignLinkTarget() to verify that the referenced object belongs to the file's trip. An authenticated user with file-edit permission on any accessible trip can submit a foreign reservation identifier through POST /api/trips/:tripId/files/:id/link, POST /api/trips/:tripId/files, or PUT /api/trips/:tripId/files/:id. Subsequent reads through FILE_SELECT or getFileLinks() join the foreign reservation and return reservation_title, disclosing reservation existence and titles across private trip boundaries. This issue is fixed in version 3.1.3.	2026-08-20	4.3	CVE-2026-62945
metaphorcreations--Post Duplicator	The Post Duplicator plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `duplicate_post()` function in all versions up to, and including, 3.0.11. This is due to the function not verifying that the user has `edit_others_posts` capability before accepting a `selectedAuthorId` parameter via the `duplicate-post` REST endpoint. This makes it possible for authenticated attackers, with Contributor-level access and above, to create duplicated posts attributed to any user, including administrators.	2026-08-22	4.3	CVE-2026-4244
metaphorcreations--Post Duplicator	The Post Duplicator plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.0.11. This is due to the	2026-08-22	4.3	CVE-2026-4245

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`duplicate_post_permissions()` permission callback only verifying the `duplicate_posts` capability without checking whether the requesting user holds `publish_posts` or other status-gated capabilities. This makes it possible for authenticated attackers, with Contributor-level access and above, to create duplicate posts with `future` (scheduled, auto-publishes) or `private` status, bypassing editorial review. Additionally, the REST endpoint does not enforce administrator-configured post-type duplication restrictions, allowing duplication of post types that have been explicitly disabled.			
michaelsweet--pdfio	PDFio before 1.6.5 contains a dangling pointer vulnerability in the dictionary string-formatting function that stores a pointer to a stack-local buffer in the document dictionary without copying the string value. In multi-threaded or pooled-request environments, attackers or concurrent users can trigger stack memory reuse across requests, causing cross-tenant document content corruption by silently overwriting one caller's dictionary string values with another caller's data.	2026-08-21	6.5	CVE-2026-77220
Microsoft--Microsoft 365 Apps for Enterprise	Improper input validation in Microsoft Office Word allows an unauthorized attacker to disclose information over a network.	2026-08-20	6.5	CVE-2026-70105
Microsoft--Windows App for Mac	Out-of-bounds read in Remote Desktop Client allows an unauthorized attacker to disclose information over a network.	2026-08-19	6.5	CVE-2026-69550
Microsoft--Windows Remote Help	Uncontrolled search path element in Windows Remote Help allows an authorized attacker to deny service locally.	2026-08-20	5.5	CVE-2026-55015
mlflow--mlflow	MLflow is an open source AI engineering platform for agents, large language models, and machine learning models. From 3.13.0 until 3.15.0, LogInputs is absent from BEFORE_REQUEST_HANDLERS in the mlflow/server/auth package, allowing any authenticated user to call POST /api/2.0/mlflow/runs/log-inputs for another user's run_id and inject attacker-controlled DatasetInput records into the dataset_inputs lineage metadata without UPDATE permission. This issue is fixed in version 3.15.0.	2026-08-17	6.5	CVE-2026-69146
MobSF--Mobile-Security-Framework-MobSF	MobSF is a mobile application security testing tool used. Prior to 4.5.1, mobsf/MobSF/settings.py places django.middleware.csrf.CsrfViewMiddleware only in the deprecated MIDDLEWARE_CLASSES setting and omits it from the active MIDDLEWARE tuple, allowing a remote attacker to make a logged-in victim submit cross-site POST requests to authenticated web endpoints including /delete_scan/, /upload/, /download_scan/, /change_password/, /create_user/, and /delete_user/. This can delete scans, upload or download applications, change passwords, or manage users with the victim account permissions. This issue is fixed in version 4.5.1.	2026-08-18	6.5	CVE-2026-68923
MobSF--Mobile-Security-Framework-MobSF	MobSF is a mobile application security testing tool used. Prior to 4.5.1, find_icon_path_zip in mobsf/StaticAnalyzer/views/android/icon_analysis.py uses the Android manifest android:icon value to construct paths under the scan resource directory without rejecting traversal or verifying containment, allowing an authenticated user to upload a crafted ZIP or APK that reads a server file with an ALLOWED_EXTENSIONS suffix, copies it to DWD_DIR as the predictable name - icon., and retrieves it through the /download/ endpoint. The same behavior provides a file-existence oracle through the icon_path report field. This issue is fixed in version 4.5.1.	2026-08-18	5.5	CVE-2026-68922
MobSF--Mobile-Security-Framework-MobSF	MobSF is a mobile application security testing tool used. Prior to 4.5.1, the unzip function in mobsf/StaticAnalyzer/views/common/shared_func.py logs that an archive member exceeding ZIP_MAX_UNCOMPRESSED_FILE_SIZE is being skipped but does not continue to the next member, so an authenticated user can upload a crafted ZIP or APK whose oversized member is extracted to disk when the	2026-08-18	4.9	CVE-2026-68924

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	aggregate ZIP_MAX_UNCOMPRESSED_TOTAL_SIZE limit has not yet been reached, potentially exhausting disk space and preventing further scans. This issue is fixed in version 4.5.1.			
mruby--mruby	A flaw has been found in mruby 3.1.0. Affected is the function udiv of the file bigint.c. Executing a manipulation can lead to floating point comparison with incorrect operator. It is possible to launch the attack remotely. The exploit has been published and may be used. It is best practice to apply a patch to resolve this issue.	2026-08-19	5.3	CVE-2022-4996
msgpack--msgpack-c	msgpack_unpacker_expand_buffer in src/unpack.c, reached through the public msgpack_unpacker_reserve_buffer API, computes its new buffer size using an unchecked size_t addition of the requested size and the amount already used. The doubling loop guards its own multiplication against overflow, but the addition in the loop condition is unguarded, so a request near SIZE_MAX wraps: the loop condition is already satisfied, the allocation is performed at the small pre-wrap size, and the function returns true. The caller is told the requested capacity was reserved when it was not, so a subsequent write of the requested length overflows the heap buffer. The library's own example/lib_buffer_unpack.c demonstrates the reserve-then-write pattern, and its defensive assert comparing capacity against the request is compiled out under NDEBUG. msgpack-c's own decode entry points do not derive the reservation size from untrusted input, so reaching this requires an integration that passes an attacker-influenced length to the reservation API, such as a length-prefixed streaming transport.	2026-08-20	5.3	CVE-2026-72854
MultiVendorX--MultiVendorX	Unauthenticated Broken Access Control in MultiVendorX <= 5.0.14 versions.	2026-08-18	6.5	CVE-2026-66651
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the calendar module does not verify private event status consistently, allowing users with viewing and moderation permissions to access and moderate private events. The private-event check used by get_events() in inc/functions_calendar.php and the event action is missing from the remaining calendar.php actions, despite the limited-access behavior described in inc/languages/english/calendar.lang.php. This issue is fixed in version 1.8.40.	2026-08-18	5.4	CVE-2026-45120
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the Email User controller does not sanitize sender names correctly, resulting in mail header injection. member.php?action=do_emailuser accepts the fromname HTTP parameter for guests or the stored username for authenticated users when the cansendemail group permission is enabled. When mail_handler is set to the default PHP mail value, the sender name is used without sanitization in Return-Path and Reply-To headers, allowing arbitrary headers to be injected with CRLF sequences. This issue is fixed in version 1.8.40.	2026-08-18	5.3	CVE-2026-45125
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the built-in CAPTCHA does not consistently enforce single-use semantics, allowing remote attackers to bypass CAPTCHA controls through challenge replay. The successful validation paths in contact.php, member.php?action=do_resendactivation, member.php?action=do_lostpw, member.php?action=do_emailuser, and sendthread.php?action=do_sendtofriend do not call captcha::invalidate_captcha() for the MyBB Default CAPTCHA selected by the captchaimage setting. A valid response can therefore be reused until a non-vulnerable endpoint invalidates it, an incorrect response is submitted, or the challenge expires. This issue is fixed in version 1.8.40.	2026-08-18	5.3	CVE-2026-45734
mybb--mybb	#### Impact The registration component does not validate the text-based _Security Question_ CAPTCHA correctly, allowing attackers to bypass the challenge via a specially crafted value. [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N) #### Details The public	2026-08-18	5.3	CVE-2026-46482

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	_Registration_workflow ([member.php?action=do_register])(https://github.com/mybb/mybb/blob/mybb_1839/member.php#L262-L307)) accepts a hidden field 'question_id' - expected to match the question session identifier ('mybb_questionsessions.sid') - and validates the challenge answer without a fail-closed fallback for invalid identifiers. If the value is blank, forged, or expired, the request continues without a question-related error. ### Patches MyBB 1.8.(...) resolves this issue with the following changes: - Commit: https://github.com/mybb/mybb/commit/ - '.patch': https://github.com/mybb/mybb/commit/.patch ### References - Release Notes: https://mybb.com/versions/1.8.(...)/ ### For more information Go to mybb.com/security to report possible security concerns or to learn more about security research at MyBB. ### Contact The security team can be reached at security@mybb.com.			
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the Admin CP UTF-8 Conversion module does not validate certain requests correctly, allowing same-site attackers to alter table encoding and deny service with a specially crafted URL. The do=all control flow in admin/modules/tools/system_health.php performs ALTER TABLE operations, column rewrite phases, and fulltext index rebuilds on GET requests for the database table named by the table parameter without request verification. The uniquely identifying implementation details include GET requests without request verification. This issue is fixed in version 1.8.40.	2026-08-18	4.6	CVE-2026-45119
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the calendar module does not check permissions consistently when listing calendars, allowing authenticated users to access titles of calendars that are otherwise inaccessible. The affected calendar-selection paths in calendar.php perform permission checks against an invalid calendar context before returning calendar titles. The uniquely identifying implementation details include titles of inaccessible calendars, and invalid calendar permission context. This issue is fixed in version 1.8.40.	2026-08-18	4.3	CVE-2026-45121
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the calendar module does not validate moderation permissions for the destination calendar when moving events. A user with moderation permission for the source calendar can move an event to a calendar where the user has only viewing permission because the do_move action in calendar.php does not check canmoderateevents for the target calendar. The uniquely identifying implementation details include calendar event move, source calendar moderation permission, and destination calendar viewing permission. This issue is fixed in version 1.8.40.	2026-08-18	4.3	CVE-2026-45122
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the remote requests feature does not correctly handle IPv6 addresses, resulting in a server-side request forgery vulnerability. The default disallowed remote hosts list does not include IPv6 addresses. Verification in fetch_remote_file() fails open when get_ip_by_hostname() returns no result because that function does not return IPv6 results, allowing a crafted remote target to bypass the host restriction. The uniquely identifying implementation details include fail-open verification, and inc/functions.php. This issue is fixed in version 1.8.40.	2026-08-18	4.3	CVE-2026-45123
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the Mod CP Report Center does not check permissions consistently, allowing moderators without report-management permission to mark reports as resolved. The modcp.php?action=do_reports Mark Selected as Read handler is reachable with canmodcp even without canmanagereportedcontent or canmanagereportedposts. When no forums are in scope, \$list_reports is empty and the UPDATE mybb_reportedcontent query executes without the expected permission-based limitation. This issue is fixed in version 1.8.40.	2026-08-18	4.3	CVE-2026-45124
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the Admin CP Recovery Codes module does not validate requests correctly, allowing same-site	2026-08-18	4.6	CVE-2026-45129

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to rotate a victim administrator's recovery codes with a specially crafted URL. The Admin CP Home, Preferences, Recovery Codes action=recovery_codes page regenerates Two-Factor Authentication recovery codes in mybb_adminoptions.recovery_codes on GET requests without request forgery protection. The uniquely identifying implementation details include admin/modules/home/preferences.php. This issue is fixed in version 1.8.40.			
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the User CP Buddy/Ignore List component does not validate reciprocal buddy-list updates correctly. The usercp.php?action=do_editlists delete handler removes the selected entry from the acting user's list and then updates mybb_users.buddylist for the target account. The reciprocal update searches for the deleted target UID instead of the acting user's UID and uses the unchecked array_search() return value as an array key. A false result can be converted to index 0, removing the target account's first stored buddy while leaving the actual reciprocal entry unchanged. The uniquely identifying implementation details include false converted to index 0. This issue is fixed in version 1.8.40.	2026-08-18	4.3	CVE-2026-47245
myCred--myCred	The myCred WordPress plugin before 3.2.5 does not verify that the receiver of an incoming payment gateway notification matches the site's configured merchant account, allowing unauthenticated attackers to have arbitrary amounts of the site's in-site currency credited to an account by completing a payment for the expected amount to a gateway account they control rather than the site's.	2026-08-21	5.3	CVE-2026-15150
myCred--New User Approve	Missing Authorization vulnerability in myCred New User Approve allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects New User Approve: from n/a through 3.2.8.	2026-08-20	5.3	CVE-2026-28163
MyThemeShop--WP Tab Widget	Contributor Cross Site Scripting (XSS) in WP Tab Widget <= 1.2.11 versions.	2026-08-18	6.5	CVE-2026-66646
NationalSecurityAgency--ghidra	Ghidra before 12.1.3 contains an uncontrolled resource consumption vulnerability in the PDB parser that allows attackers to terminate the Ghidra process by supplying a crafted PDB file with an oversized parameters section. The AbstractPdb deserialization routine reads all remaining parameters into an unbounded list, causing uncontrolled heap growth that triggers an OutOfMemoryError which bypasses exception handling and crashes the application.	2026-08-20	5.5	CVE-2026-54389
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.2, lemur/certificates/verify.py accepted CRL Distribution Point and OCSP responder URLs from uploaded certificate extensions and used them in crl_verify and ocsf_verify without adequate destination validation. An authenticated operator could submit a certificate through POST /api/1/certificates/upload and cause verify_string to reach loopback, RFC1918, link-local, or instance-metadata destinations such as 169.254.169.254. The requests could probe internal services and create side effects from the Lemur host network position. The CRL path also used an unbounded cache, allowing attacker-controlled entries to persist and consume memory. The fix validates destinations, supports explicit trusted-host allowlists, and bounds the CRL cache. This issue is fixed in version 1.9.2.	2026-08-18	6.3	CVE-2026-55162
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.2, PUT /api/1/roles/ in lemur/roles/views.py:298 authorized updates with RoleMemberPermission(role_id), which allowed either an administrator or any existing member of the target role. The handler passed data["users"] and data["name"] to service.update, allowing a non-admin member to add or remove other users and rename the role. This enabled lateral privilege grants within roles that control certificate and authority access and could deny access by removing legitimate members. The DELETE handler already required admin_permission, confirming that the weaker PUT authorization was inconsistent. The fix applies the same administrator-only requirement to the PUT handler. This issue is fixed in version 1.9.2.	2026-08-18	6.3	CVE-2026-55163

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.3, <code>_validate_revocation_url</code> in <code>lemur/certificates/verify.py</code> checked the original CRL or OCSP URL but the later request could reach a different destination. The CRL requests.get call followed HTTP redirects without validating each Location target, so a public attacker-controlled URL could redirect to loopback, RFC1918, link-local, or instance-metadata addresses. Validation and connection also performed separate DNS resolutions, creating a time-of-check time-of-use window for DNS rebinding on both CRL and OCSP paths. An operator uploading a certificate through <code>POST /api/1/certificates/upload</code> could therefore induce blind internal requests despite the earlier mitigation. The fix disables redirects and pins validated addresses while preserving the correct Host value. This issue is fixed in version 1.9.3.	2026-08-18	6.3	CVE-2026-70667
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.3, <code>POST /api/1/authorities</code> with <code>type=subca</code> did not require <code>AuthorityPermission</code> on the parent authority when <code>ADMIN_ONLY_AUTHORITY_CREATION</code> was false. <code>AssociatedAuthoritySchema</code> resolved the caller-supplied parent and passed it through authority creation to <code>cryptography-issuer</code> , which used the parent <code>authority_certificate.private_key</code> to sign a new intermediate. Any authenticated non-read-only user in that supported configuration could chain a sub-CA to an internal root for which the user held no role. The resulting intermediate could issue trusted certificates and its private key could be used outside Lemur, bypassing normal issuance controls. The fix checks <code>AuthorityPermission</code> on every supplied parent before invoking the issuer. This issue is fixed in version 1.9.3.	2026-08-18	6.5	CVE-2026-71317
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.2, <code>lemur.users.service.update</code> assigned a replacement password directly to <code>users.password</code> , while <code>lemur/users/models.py</code> registered <code>User.hash_password</code> only for the <code>before_insert</code> event. Because no <code>before_update</code> listener ran, administrator-initiated password changes through <code>PUT /api/1/users/</code> were committed as plaintext. The affected user could no longer authenticate normally because <code>bcrypt</code> verification received an unhashed value. A database, backup, replica, query-log, or administrative read compromise exposed immediately usable credentials without offline cracking. The fix registers hashing for <code>before_update</code> and avoids rehashing values that already have a <code>bcrypt</code> prefix. This issue is fixed in version 1.9.2.	2026-08-18	4.9	CVE-2026-55164
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.2, the JWT verifier in <code>lemur/auth/service.py:130-137</code> used <code>fetch_token_header</code> to read <code>header_data["alg"]</code> from an unverified token and passed that attacker-controlled value to <code>decode_with_multiple_secrets</code> . <code>PyJWT 2.x</code> rejects <code>alg=none</code> with the configured key, so the flaw is a defense-in-depth gap rather than a direct authentication bypass in the shipped configuration. The unpinned algorithm can become exploitable after an asymmetric-signing migration through algorithm confusion, and it weakens algorithm-based anomaly detection because the token chooses the recorded value. A separate disclosure of <code>LEMUR_TOKEN_SECRET</code> would also permit forged HS256 tokens, although that disclosure is an independent prerequisite. The fix introduces the server-controlled <code>LEMUR_TOKEN_ALGORITHMS</code> allowlist and defaults it to HS256. This issue is fixed in version 1.9.2.	2026-08-18	4.8	CVE-2026-55165
Netflix--lemur	Lemur manages TLS certificate creation. Prior to 1.9.3, <code>CertificateExport</code> placed its <code>CertificatePermission</code> ownership check inside the <code>plugin.requires_key</code> branch for <code>POST /api/1/certificates/export</code> . A plugin declaring <code>requires_key</code> false bypassed that check, and the handler still passed <code>cert.private_key</code> as an argument and recorded a <code>key_view</code> audit event. The bundled <code>JavaTruststoreExportPlugin</code> ignored the key, so the immediate exposure was limited to public certificate material and misleading audit entries, but a future plugin could have consumed the supplied key. The fix passes no private key to plugins that do not require one and confines ownership checks and <code>key_view</code> logging to actual private-key exports. This issue is fixed in version 1.9.3.	2026-08-18	4.3	CVE-2026-71322

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Netgate--pfSense Plus	pfSense Plus before 26.07 and pfSense CE through 2.8.1 contain a stored cross-site scripting vulnerability in the Traffic Graphs top-talkers feature, where PTR records returned by reverse DNS lookups are incorporated without sanitization into AJAX responses and rendered as HTML through a DOM sink in the administrator interface. An attacker who controls a PTR record and generates sufficient traffic to appear as a top talker can execute arbitrary JavaScript in an administrator's browser, gaining access to the authenticated session context and same-origin access to the firewall management interface, enabling account creation and arbitrary OS command execution.	2026-08-19	6.1	CVE-2026-67189
Netiket Information Technologies--EdoWEB	Authorization bypass through User-Controlled key vulnerability in Netiket Information Technologies EdoWEB allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects EdoWEB: before 780-g7.	2026-08-18	5.3	CVE-2026-16309
netty--netty	Netty is an asynchronous, event-driven network application framework. Prior to 4.1.137.Final and 4.2.17.Final, io.netty.handler.codec.http.cors.CorsHandler setVaryHeader replaces application Vary headers such as Authorization or Cookie with Origin, allowing a caching proxy or CDN to reuse authenticated responses across users and disclose sensitive information. This issue is fixed in versions 4.1.137.Final and 4.2.17.Final.	2026-08-17	6.5	CVE-2026-59903
Nexcess--GiveWP	Unauthenticated Broken Access Control in GiveWP < 4.16.6 versions.	2026-08-18	6.5	CVE-2026-73348
Nexcess--GiveWP	Unauthenticated Broken Access Control in GiveWP <= 4.16.5.1 versions.	2026-08-18	6.5	CVE-2026-73352
next-terminal--next-terminal	Next Terminal fails to enforce per-asset authorization checks on the portal ping and wake-on-LAN endpoints, allowing any authenticated user to probe and wake assets they are not granted access to. Attackers can call these endpoints with arbitrary asset identifiers to retrieve asset information including display names, reachability status, connection timing, and network addresses, or trigger wake-on-LAN packets on unauthorized assets.	2026-08-17	5.4	CVE-2026-75108
nicolargo--glances	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.6, the cors_origins guard in glances/outputs/glances_restful_api.py uses exact list equality instead of wildcard membership, allowing a multi-origin list containing the wildcard to retain cors_credentials and expose authenticated REST API data to an untrusted website visited by a previously authenticated user. This issue is fixed in 4.5.6.	2026-08-17	6.5	CVE-2026-68517
nicolargo--glances	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.6, as_dict_secure() in glances/config.py checks only option names and exposes public_username and credentials embedded in public_api values through unauthenticated GET /api/4/config and GET /api/4/config/ip requests. This issue is fixed in 4.5.6.	2026-08-17	5.3	CVE-2026-68520
nlTK--nlTK	NLTK versions before 3.10.0 contain a logic bug in FileSystemPathPointer.open() where the sandbox validation check compares a normalized path against itself, making the security check permanently inert. Attackers can pass file:// URLs to nlTK.data.load() to read arbitrary files accessible to the process user, including credentials and configuration files.	2026-08-22	6.5	CVE-2026-65915
nlTK--nlTK	NLTK versions before 3.9.4 contain a symlink escape vulnerability in CorpusReader.open() that allows local attackers to read arbitrary files outside the corpus root. The vulnerability exists because path validation is lexical and does not account for symlink resolution, enabling attackers to place symlinks inside the corpus root to access files outside the intended boundary.	2026-08-22	6.2	CVE-2026-70626
nlTK--nlTK	nlTK versions before 3.10.2 contain a symlink-based arbitrary file read vulnerability in IPIPANCorpusReader methods that bypass nlTK.pathsec validation entirely. Attackers can place a symlink in the corpus root directory and read arbitrary files	2026-08-22	5.5	CVE-2026-62383

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accessible to the process by calling channels(), domains(), categories(), or fileids() methods with the symlink filename.			
nlTK--nlTK	NLTK versions before 3.10.0 contain a path traversal vulnerability in FramenetCorpusReader and NKJPCorpusReader that allows attackers to parse XML files outside the corpus root by supplying unsafe selectors or poisoned index state. Attackers can exploit frame_by_name, doc, lu, and header methods with crafted parameters to read arbitrary XML files accessible to the application.	2026-08-22	5.9	CVE-2026-62385
nlTK--nlTK	NLTK before 3.10.0 (affected versions <= 3.9.4) contains a server-side request forgery (SSRF) vulnerability in the validate_network_url() function in nlTK/pathsec.py. The _resolve_hostname() helper catches OSError and ValueError during socket.getaddrinfo() and returns an empty list; when DNS resolution fails, the validation loop executes no IP checks and the function fails open, allowing urlopen() to proceed without validation. An attacker who can trigger DNS resolution failures or use DNS rebinding can bypass SSRF protections and reach restricted network resources, including cloud metadata endpoints (e.g., 169.254.169.254).	2026-08-22	5.3	CVE-2026-63311
nosilver4u--EWWW Image Optimizer	The EWWW Image Optimizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'data-script' Lazy Load Attribute in Post Content in all versions up to, and including, 8.7.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit is achieved by embedding a crafted img element with class='lazyload' and a data-script attribute pointing to an attacker-controlled URL in post content, which the plugin's bundled lazysizes ls.unveilhooks addon then uses to dynamically create and insert a script element into the DOM at page view time.	2026-08-19	6.4	CVE-2026-15446
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker could cause an absolute path traversal. A successful exploit might lead to code execution and information disclosure.	2026-08-18	6.5	CVE-2026-47606
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker could cause an absolute path traversal. A successful exploit might lead to code execution.	2026-08-18	5.5	CVE-2026-47630
OliveTin--OliveTin	OliveTin gives access to predefined shell commands from a web interface. The 'filterToDefinedArgumentsOnly' function in the executor is intended to discard any arguments not explicitly defined in the action's configuration. However, prior to commit ebffd9f040f791208aee1db2e5a8aecd1e3e603d, a special case allows any argument whose name starts with 'ot_' to bypass this filter. While two system arguments ('ot_executionTrackingId' and 'ot_username') are injected by OliveTin and overridden, all other 'ot_'-prefixed arguments supplied by the user pass through unmodified. These bypassed arguments are not type-checked - the validation loop only iterates over the action's defined arguments, so 'ot_'-prefixed arguments skip all type safety checks entirely; set as environment variables - via 'buildEnv()', with completely unvalidated values, and passed to the executed command; and included in the template context - available as '.Arguments.ot_*' in template rendering. Commit ebffd9f040f791208aee1db2e5a8aecd1e3e603d contains a patch.	2026-08-21	4.3	CVE-2026-53541
omnivore-app--omnivore	The scanFeedsResolver in packages/api/src/resolvers/subscriptions/index.ts passes the caller-supplied url straight to axios.get(url, rssParserConfig()) with no address validation. The same file guards the subscribe path with validateUrl(), which rejects private and reserved ranges through the private-ip library, and createPageSaveRequest applies the same check, so the omission is specific to this resolver. An authenticated user can direct the server to request arbitrary internal endpoints. The response is parsed as a feed or as HTML and the resolver returns the resulting url, title, description and type fields, so disclosure is limited to feed-	2026-08-20	5	CVE-2026-77066

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	shaped metadata and to link elements advertising RSS or Atom feeds; requests that do not parse still distinguish reachable ports from unreachable ones through the resulting error.			
omnivore-app--omnivore	The setWebhookResolver in packages/api/src/resolvers/webhooks/index.ts stores the caller-supplied url without any address validation, and the file imports no validation helper. When a subscribed event fires, callWebhook in packages/api/src/jobs/call_webhook.ts issues axios.request with that url, the method and Content-Type recorded on the webhook, and a JSON body carrying the event data, so an authenticated user can make the server send repeated attacker-shaped requests to internal endpoints, including link-local metadata addresses. The request is blind: callWebhook discards the result and writes only a success line or the axios error to the server log, so the response is not returned through the API.	2026-08-20	5	CVE-2026-77067
ondata--ckan-mcp-server	CKAN MCP Server is a tool for querying CKAN open data portals. A known vulnerability CVE-2026-33060 indicated tools including ckan_package_search and sparql_query that accept a base_url parameter had the risk of making HTTP requests to arbitrary endpoints without restriction. A fix was applied to filter out ip addresses. However, a method to bypass exists prior to version 0.4.106. CKAN MCP Server validates caller-supplied CKAN server URLs by inspecting only the parsed hostname string before issuing outbound HTTP requests. In `src/utlis/http.ts`, hostname aliases such as `ip6-localhost` are not equal to `localhost`, are not dotted IPv4 literals, and are not bracketed IPv6 literals, so they pass the SSRF filter but can resolve to loopback when the server performs the request. A remote MCP caller that can invoke CKAN tools with a `server_url` can therefore make the server connect to local or private addresses and, for CKAN-shaped responses, receive response-derived data. The updated fix in version 0.4.106 replaced the single `hostname === 'localhost'` check with a blocked-hostname `Set` covering `ip6-localhost` and `ip6-loopback`.	2026-08-21	5.7	CVE-2026-53509
onyx-dot-app--onyx	Onyx is an open-source AI platform. Prior to 4.3.0, Onyx Enterprise Edition's PATCH /manage/admin/user-group/{user_group_id} and POST /manage/admin/user-group/{user_group_id}/add-users endpoints in ee/onyx/server/user_group/api.py call update_user_group and add_users_to_user_group in ee/onyx/db/user_group.py without enforcing _validate_curator_can_modify_group, allowing a curator to add accounts to arbitrary groups and obtain document access through get_acl_for_user and the OpenSearch access_control_list filter. This issue is fixed in version 4.3.0.	2026-08-17	6.5	CVE-2026-63178
Open Asset Import Library Assimp--Assimp	A security vulnerability has been detected in Open Asset Import Library Assimp 17c12da. The affected element is the function Assimp::MDLImporter::ParseBoneTrafoKeys_3DGS_MDL7 of the file code/AssetLib/MDL/MDLLoader.cpp of the component 3DGS MDL7 Bone Transformation Key Parser. The manipulation of the argument transmatrix_count/pcBoneTransforms leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The identifier of the patch is 50d767984e78d51b53e2020fdf0967fd624bc377. It is recommended to apply a patch to fix this issue.	2026-08-17	6.3	CVE-2026-19999
Open Asset Import Library--Assimp	A security flaw has been discovered in Open Asset Import Library Assimp 17c12da. Impacted is the function Assimp::Compression::decompressBlock of the file code/Common/Compression.cpp of the component File Parser. Performing a manipulation results in heap-based buffer overflow. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-17	6.3	CVE-2026-19967
Open Asset Import Library--Assimp	A vulnerability was detected in Open Asset Import Library Assimp 17c12da. This affects the function Assimp::MDLImporter::AddBonesToNodeGraph_3DGS_MDL7 of the file code/AssetLib/MDL/MDLLoader.cpp of the component Node Parser. The	2026-08-17	6.3	CVE-2026-19970

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manipulation of the argument bones_num results in heap-based buffer overflow. The attack can be executed remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.			
Open Asset Import Library--Assimp	A security vulnerability has been detected in Open Asset Import Library Assimp 17c12da. The impacted element is the function Assimp::MDLImporter::GenerateOutputMeshes_3DGS_MDL7 of the file code/AssetLib/MDL/MDLLoader.cpp of the component 3DGS MDL7 Model Output Mesh Generator. The manipulation leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-17	5.4	CVE-2026-19969
Open Asset Import Library--Assimp	A weakness has been identified in Open Asset Import Library Assimp 17c12da. The affected element is the function Assimp::MDLImporter::ReadFaces_3DGS_MDL7 in the library code/AssetLib/LWO/LWOLoader.h of the component 3DGS MDL7 Model Parser. Executing a manipulation can lead to heap-based buffer overflow. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. This patch is called ee77bb09a42a49843ac85ef64c14d2328b251df1. Applying a patch is advised to resolve this issue.	2026-08-17	4.3	CVE-2026-19968
OpenBoxes--OpenBoxes	A weakness has been identified in OpenBoxes up to 0.9.2. This vulnerability affects unknown code of the file rails-app/controllers/org/pih/warehouse/RoleInterceptor.groovy of the component Product Supplier Edit Controller. Executing a manipulation can lead to improper authorization. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. Upgrading to version 0.9.3 is able to resolve this issue. This patch is called f767ac1a5987d4865d9f158c6a967680f8e45468. It is suggested to upgrade the affected component.	2026-08-18	6.3	CVE-2024-14045
OpenBoxes--OpenBoxes	A security vulnerability has been detected in OpenBoxes up to 0.9.1. This issue affects the function DocumentController of the file rails-app/controllers/org/pih/warehouse/core/DocumentController.groovy of the component Document Upload Controller. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 0.9.2 is capable of addressing this issue. The identifier of the patch is e945d6bfcec29642f514e7d298dfba2cc6cd7cd4. Upgrading the affected component is recommended.	2026-08-18	6.3	CVE-2024-14046
openemr--openemr	OpenEMR before 8.2.0 contains a path traversal vulnerability in the standard_tables_manage.php interface where the db GET parameter is passed without validation to temp_dir_cleanup(), which joins the value to the PHP temporary directory path and recursively deletes the resulting directory. Attackers can supply a traversal sequence in the db parameter to resolve outside the intended temporary directory, and by chaining this with an open redirect in dicom_frame.php, an unauthenticated attacker can deliver a crafted URL that triggers arbitrary recursive directory deletion within an authenticated Superuser's session.	2026-08-17	6.5	CVE-2026-40506
openemr--openemr	OpenEMR before 8.3.0 contains a reflected cross-site scripting vulnerability in the patient portal template import handler. The templateHtml GET parameter is reflected into the page response without sanitization. An attacker can craft a URL that executes arbitrary JavaScript in the browser of any authenticated user with Forms Administration permissions who visits the link, enabling session hijacking.	2026-08-19	6.1	CVE-2026-40507
openemr--openemr	OpenEMR before 8.3.0 contains a stored cross-site scripting vulnerability in the patient portal template import handler that allows authenticated attackers with Forms Administration permissions to upload template files containing arbitrary	2026-08-19	5.4	CVE-2026-40508

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTML or JavaScript. Attackers can inject malicious scripts through the template upload functionality, which are stored without sanitization and execute in the browser of any other Forms Administration user who views the template in the HTML editor.			
openemr--openemr	OpenEMR before 8.3.0 contains a cross-site request forgery vulnerability in the DICOM viewer. The web_path GET parameter in the DICOM viewer page is embedded unsanitized as a URL without validation against expected path formats. An attacker can craft a URL that causes an authenticated user with Patients - Documents permissions to make authenticated requests to arbitrary OpenEMR endpoints, enabling forced logout and other state-changing actions.	2026-08-19	4.3	CVE-2026-40509
openemr--openemr	OpenEMR before 8.3.0 contains a path traversal vulnerability in the EDI archive restore function. The archrestore_sel POST parameter is passed to the archive restore handler without sanitization for path traversal sequences. The handler checks whether the supplied path exists on the filesystem, and the differing response messages leak whether the target path exists. An authenticated user with EOB Data Entry permissions can probe arbitrary filesystem paths on the server to determine file existence.	2026-08-19	4.3	CVE-2026-76614
OpenListTeam--OpenList	OpenList a file list program that supports multiple storage. Prior to 4.2.4, the share creation and update checks in server/handles/sharing.go use strings.HasPrefix(requested_path, user.BasePath) without enforcing a directory separator boundary. An authenticated user with CanShare permission and a BasePath such as /base can submit a sibling path such as /base2/secret.txt, create a share for the out-of-scope file, and use the public share download or list handlers to read data outside the assigned directory. This issue is fixed in version 4.2.4.	2026-08-18	6.5	CVE-2026-69160
Openpanel-dev--openpanel	The report.get procedure in packages/trpc/src/routers/report.ts accepted only a reportId and returned getReportById(reportId) directly. The enforceAccess middleware in packages/trpc/src/trpc.ts evaluates membership only when the input carries a projectId or organizationId key, so an input consisting of a reportId alone passed through unchecked, and getReportById in packages/db/src/services/reports.service.ts performs a findUnique on the report id with no project scoping. Any authenticated user could therefore read the full configuration of any saved report on the instance, including the owning projectId, event series, filters, breakdowns and formulas, by supplying its identifier. The adjacent update, delete and duplicate procedures resolve the report first and check getProjectAccess against the report's own projectId, so the omission was specific to this procedure.	2026-08-21	6.5	CVE-2026-77768
Openpanel-dev--openpanel	The report.list procedure in packages/trpc/src/routers/report.ts accepted a projectId and a dashboardId and returned getReportsByDashboardId(dashboardId). The enforceAccess middleware in packages/trpc/src/trpc.ts verified membership for the supplied projectId, but nothing verified that the supplied dashboardId belonged to that project, and getReportsByDashboardId in packages/db/src/services/reports.service.ts selects reports by dashboardId alone with no project scoping. An authenticated user could therefore pair a projectId from their own organization, which satisfies the middleware, with a dashboardId belonging to another organization and receive every report in that dashboard. A correctly scoped helper, listReportsCore, already existed in the same service file and resolves the dashboard through getDashboardById(dashboardId, projectId) before returning reports, but the router did not use it.	2026-08-21	6.5	CVE-2026-77769
openwrt--luci	luci-lib-px5g (LuCI) contains a heap-based buffer overflow in the native ASN.1 encoding routine asn1_add_obj (x509write.c) when signing a certificate with a 2040-bit RSA key. For a 255-byte signature, the BIT STRING allocation is computed from the DER length encoding of 255 bytes, but the payload written after prepending the unused-bits byte is 256 bytes, requiring one additional DER length octet. As a result the allocation is 259 bytes while the tag, length, unused-bits byte, and signature require 260 bytes, and the final memcpy writes one byte beyond the	2026-08-22	6.6	CVE-2026-62381

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	heap buffer. The overflow is reachable through the exported Lua interface via create_selfsigned(); whether it is remotely exploitable depends on the embedding application. The vulnerable code is present on the openwrt-18.06 through openwrt-25.12 release branches and is absent from master, where the luci-lib-px5g package has been removed rather than patched.			
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-70923
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. While the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.8	CVE-2026-71029
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Helidon executes to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data as well as unauthorized update, insert or delete access to some of Helidon accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	6.1	CVE-2026-71154
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data as well as unauthorized update, insert or delete access to some of Helidon accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	6.5	CVE-2026-71162
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	6.5	CVE-2026-73867
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1	2026-08-18	6.5	CVE-2026-73868

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).			
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-73869
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-73870
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	6.5	CVE-2026-73892
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	6.5	CVE-2026-73893
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP/2 to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2026-08-18	6.5	CVE-2026-73896
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	6.5	CVE-2026-73897

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Helidon, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-73898
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	6.5	CVE-2026-73904
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2026-08-18	6.5	CVE-2026-73914
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Helidon accessible data. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	2026-08-18	5.9	CVE-2026-70716
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-70727
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	2026-08-18	5.3	CVE-2026-71156
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-71157

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2026-08-18	5.3	CVE-2026-71161
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	5.4	CVE-2026-71165
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73871
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73872
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	5.4	CVE-2026-73874
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73877
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	5.4	CVE-2026-73881

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73888
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73889
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73895
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73899
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73900
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-73906
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	5.9	CVE-2026-73909
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base	2026-08-18	5.3	CVE-2026-73910

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	5.4	CVE-2026-73911
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	5.4	CVE-2026-73913
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	5.4	CVE-2026-73919
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Helidon. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2026-08-18	5.3	CVE-2026-73932
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.18. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	4.2	CVE-2026-73873
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Helidon executes to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Helidon accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	4.4	CVE-2026-73880
Oracle Corporation-- Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 4.5.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data as well as unauthorized read access to a subset of Helidon accessible data. CVSS 3.1	2026-08-18	4.8	CVE-2026-73901

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).			
Oracle Corporation--MySQL Connectors	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). The supported version that is affected is 26.7.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	6.5	CVE-2026-71079
Oracle Corporation--MySQL Connectors	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). The supported version that is affected is 26.7.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors and unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H).	2026-08-18	6.8	CVE-2026-71084
Oracle Corporation--MySQL Connectors	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). The supported version that is affected is 26.7.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H).	2026-08-18	5.5	CVE-2026-71073
Oracle Corporation--Oracle Access Manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authorization Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Access Manager. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2026-08-18	4.3	CVE-2026-71124
Oracle Corporation--Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Engineering Communication Interface). The supported version that is affected is 6.2.1. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Agile Engineering Data Management executes to compromise Oracle Agile Engineering Data Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Agile Engineering Data Management. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2026-08-18	6.3	CVE-2026-70693
Oracle Corporation--Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Install). The supported version that is affected is 6.2.1. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Agile Engineering Data Management executes to compromise Oracle Agile Engineering Data Management. Successful attacks of this vulnerability can result in takeover of Oracle Agile Engineering Data Management. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	6.7	CVE-2026-70698

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Install). The supported version that is affected is 6.2.1. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Agile Engineering Data Management executes to compromise Oracle Agile Engineering Data Management. Successful attacks of this vulnerability can result in takeover of Oracle Agile Engineering Data Management. CVSS 3.1 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	6.4	CVE-2026-70712
Oracle Corporation-- Oracle Agile Engineering Data Management	Vulnerability in the Oracle Agile Engineering Data Management product of Oracle Supply Chain (component: Engineering Communication Interface). The supported version that is affected is 6.2.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile Engineering Data Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile Engineering Data Management accessible data as well as unauthorized read access to a subset of Oracle Agile Engineering Data Management accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	4.8	CVE-2026-70709
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-71070
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM MCAD Connector accessible data as well as unauthorized update, insert or delete access to some of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	5.9	CVE-2026-71075
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-71076
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	5.3	CVE-2026-71077
Oracle Corporation--	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Easily	2026-08-18	5.3	CVE-2026-71087

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Agile PLM MCAD Connector	exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM MCAD Connector accessible data as well as unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Agile PLM MCAD Connector. CVSS 3.1 Base Score 4.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L).	2026-08-18	4.5	CVE-2026-71066
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM MCAD Connector accessible data as well as unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 4.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	4.6	CVE-2026-71071
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM MCAD Connector accessible data as well as unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Agile PLM MCAD Connector. CVSS 3.1 Base Score 4.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L).	2026-08-18	4.2	CVE-2026-71078
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM MCAD Connector. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N).	2026-08-18	4.8	CVE-2026-71088
Oracle Corporation-- Oracle Cash Management	Vulnerability in the Oracle Cash Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Cash Management executes to compromise Oracle Cash Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Cash Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Cash Management accessible data. CVSS 3.1 Base	2026-08-18	6	CVE-2026-70726

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 6.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.8	CVE-2026-70982
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.8	CVE-2026-70983
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Commerce Guided Search / Oracle Commerce Experience Manager executes to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70989
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.8	CVE-2026-70990
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Content Acquisition System). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Commerce Guided Search / Oracle Commerce	2026-08-18	6.3	CVE-2026-70991

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Experience Manager	Experience Manager executes to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-71001
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-71004
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-71005
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-71006

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.8	CVE-2026-71007
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. While the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.8	CVE-2026-71008
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Experience Manager). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-71011
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Commerce Guided Search / Oracle	2026-08-18	6.5	CVE-2026-71017

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Commerce Experience Manager. CVSS 3.1 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:L).			
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Internal operations). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-71019
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-71025
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Guided Search / Oracle Commerce Experience Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data as well as unauthorized read access to a subset of Oracle Commerce Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-71031
Oracle Corporation-- Oracle Commerce Guided Search / Oracle Commerce Experience Manager	Vulnerability in the Oracle Commerce Guided Search / Oracle Commerce Experience Manager product of Oracle Commerce (component: Endeca Application Controller). The supported version that is affected is 11.4.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Commerce Guided Search / Oracle Commerce Experience Manager executes to compromise Oracle Commerce Guided Search / Oracle Commerce Experience Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Commerce	2026-08-18	5.5	CVE-2026-71033

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Guided Search / Oracle Commerce Experience Manager accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Database Server	Vulnerability in the RDBMS component of Oracle Database Server. Supported versions that are affected are 19.3-19.32, 21.3-21.23 and 23.4.0-23.26.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise RDBMS. Successful attacks of this vulnerability can result in unauthorized read access to a subset of RDBMS accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-71100
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Enterprise Manager Install). Supported versions that are affected are 13.5 and 24.1. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 5.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	5.6	CVE-2026-61298
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 6.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N).	2026-08-18	6.7	CVE-2026-61313
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-62578
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	2026-08-18	5.3	CVE-2026-61342
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager.	2026-08-18	5.4	CVE-2026-62441

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Calculation Manager	Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data as well as unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).			
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-62446
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. While the vulnerability is in Oracle Hyperion Calculation Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 5.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2026-08-18	5	CVE-2026-62460
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data as well as unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	5.4	CVE-2026-62603
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Calculation Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N).	2026-08-18	5.9	CVE-2026-70677
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	2026-08-18	5.3	CVE-2026-70679
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with	2026-08-18	4.3	CVE-2026-70683

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Calculation Manager	network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).			
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 4.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N).	2026-08-18	4.1	CVE-2026-70714
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 4.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	4	CVE-2026-70719
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Data Relationship Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Data Relationship Management. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	6.6	CVE-2026-70888
Oracle Corporation-- Oracle Hyperion Data Relationship Management	Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Data Relationship Management executes to compromise Oracle Hyperion Data Relationship Management. While the vulnerability is in Oracle Hyperion Data Relationship Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Data Relationship Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70895
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70824
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical	2026-08-18	6.5	CVE-2026-70825

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Financial Management	data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70826
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70831
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	6.1	CVE-2026-70838
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	6.8	CVE-2026-70843
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70847
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management.	2026-08-18	6.5	CVE-2026-70849

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Financial Management	Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:H).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70938
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70969
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70975
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	6	CVE-2026-71013
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hyperion Financial Management as well as unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data and unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H).	2026-08-18	6.4	CVE-2026-71090
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with	2026-08-18	6.5	CVE-2026-71091

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Financial Management	network access via SQL to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2026-08-18	6.3	CVE-2026-71103
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	6.7	CVE-2026-71109
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in takeover of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	6.4	CVE-2026-71119
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	2026-08-18	6.5	CVE-2026-71121
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	5.5	CVE-2026-70836
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with	2026-08-18	5.6	CVE-2026-70841

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Financial Management	logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. While the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 5.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-70911
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:N/I:H/A:N).	2026-08-18	5.3	CVE-2026-70912
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	5.3	CVE-2026-70974
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	5.3	CVE-2026-71108
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	5.3	CVE-2026-71120
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with	2026-08-18	5.4	CVE-2026-71123

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Financial Management	network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-71148
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 4.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	4	CVE-2026-70916
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 4.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	4	CVE-2026-70917
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	4.4	CVE-2026-71060
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	4.9	CVE-2026-71085
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hyperion Financial Management. CVSS	2026-08-18	4.7	CVE-2026-71105

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3.1 Base Score 4.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	4.8	CVE-2026-71118
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	4.4	CVE-2026-71145
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 4.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L).	2026-08-18	4.2	CVE-2026-71147
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 4.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L).	2026-08-18	4.2	CVE-2026-71149
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Repository). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting	2026-08-18	6.5	CVE-2026-60682

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).			
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Reporting accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).	2026-08-18	6.8	CVE-2026-70751
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N).	2026-08-18	6.3	CVE-2026-70753
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Reporting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-70765
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70767
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Financial Reporting, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-70768

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	6.5	CVE-2026-70769
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Financial Reporting executes to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Reporting accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	6.8	CVE-2026-70780
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	6.5	CVE-2026-70788
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-70754
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Reporting executes to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:N).	2026-08-18	5.3	CVE-2026-70758
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting	2026-08-18	5.4	CVE-2026-70759

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).			
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	2026-08-18	5.4	CVE-2026-70766
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Reporting executes to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:N).	2026-08-18	5.3	CVE-2026-70784
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Financial Reporting accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 5.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N).	2026-08-18	5.9	CVE-2026-70789
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	4.2	CVE-2026-70793
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Reporting executes to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N).	2026-08-18	4.7	CVE-2026-70794
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure	2026-08-18	6.1	CVE-2026-62499

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).			
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-62506
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-62523
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via SQL to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	6.5	CVE-2026-62555
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).	2026-08-18	6.3	CVE-2026-62558
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized read access to a subset of	2026-08-18	6.1	CVE-2026-62568

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).			
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. While the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-62572
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-08-18	6.5	CVE-2026-62576
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hyperion Infrastructure Technology, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	6.1	CVE-2026-70961
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70968
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	6.8	CVE-2026-70972

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-62509
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-62510
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	5.5	CVE-2026-62553
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	5.5	CVE-2026-62564
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	5.3	CVE-2026-62566
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	5.5	CVE-2026-62573
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion	2026-08-18	5.3	CVE-2026-62579

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Infrastructure Technology	Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Events). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	4.8	CVE-2026-62520
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	4.7	CVE-2026-62575
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 4.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	4	CVE-2026-62584
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data as well as unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	4.2	CVE-2026-70963
Oracle Corporation-- Oracle Installed Base	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base accessible data as well as unauthorized read access to a subset of Oracle Installed Base accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Installed Base. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2026-08-18	6.3	CVE-2026-70775
Oracle Corporation-- Oracle Java SE,	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u501, 11.0.32, 17.0.20, 21.0.12,	2026-08-18	6.8	CVE-2026-61308

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	25.0.4, 26.0.2; Oracle GraalVM for JDK: 17.0.20 and 21.0.12; Oracle GraalVM Enterprise Edition: 21.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u501, 11.0.32, 17.0.20, 21.0.12, 25.0.4, 26.0.2; Oracle GraalVM for JDK: 17.0.20 and 21.0.12; Oracle GraalVM Enterprise Edition: 21.3.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2026-08-18	5.3	CVE-2026-70907
Oracle Corporation-- Oracle Learning Management	Vulnerability in the Oracle Learning Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Learning Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Learning Management accessible data as well as unauthorized read access to a subset of Oracle Learning Management accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	6.5	CVE-2026-61198
Oracle Corporation-- Oracle Mobile Application Server	Vulnerability in the Oracle Mobile Application Server product of Oracle E-Business Suite (component: MWA Terminal Server). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Mobile Application Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Mobile Application Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70732
Oracle Corporation-- Oracle Production Scheduling	Vulnerability in the Oracle Production Scheduling product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Production Scheduling. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Production Scheduling accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-70720
Oracle Corporation-- Oracle Public	Vulnerability in the Oracle Public Sector Financials (International) product of Oracle E-Business Suite (component: Authorization). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker	2026-08-18	6.3	CVE-2026-61139

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Sector Financials (International)	with network access via HTTP to compromise Oracle Public Sector Financials (International). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Public Sector Financials (International) accessible data as well as unauthorized read access to a subset of Oracle Public Sector Financials (International) accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Public Sector Financials (International). CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).			
Oracle Corporation-- Oracle Shipping Execution	Vulnerability in the Oracle Shipping Execution product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Shipping Execution. Successful attacks of this vulnerability can result in takeover of Oracle Shipping Execution. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-08-18	6.6	CVE-2026-62475
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Difficult to exploit vulnerability allows low privileged attacker with network access via LDAP to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Unified Directory accessible data as well as unauthorized access to critical data or complete access to all Oracle Unified Directory accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-08-18	6.8	CVE-2026-60895
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6	CVE-2026-71114
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6	CVE-2026-71115
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox as well as unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H).	2026-08-18	6.1	CVE-2026-71125
Oracle Corporation--	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily	2026-08-18	6	CVE-2026-71127

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle VM VirtualBox	exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).			
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	2026-08-18	6	CVE-2026-71128
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	2026-08-18	6	CVE-2026-71135
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	2026-08-18	6	CVE-2026-71137
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	5.3	CVE-2026-71132
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a	2026-08-18	5.7	CVE-2026-71134

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 5.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L).			
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 5.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/H/I:N/A:N).	2026-08-18	5.6	CVE-2026-71151
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2026-08-18	4.4	CVE-2026-71139
Oracle Corporation-- Oracle Workflow	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Worklist). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Workflow. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Workflow accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-08-18	6.5	CVE-2026-60830
Oracle Corporation-- PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Panel Processor). Supported versions that are affected are 8.61-8.63. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N).	2026-08-18	4.4	CVE-2026-60884
Oracle Corporation-- Service Delivery Platform	Vulnerability in the Service Delivery Platform product of Oracle Fusion Middleware (component: Messaging Enabler). Supported versions that are affected are 14.1.2.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Service Delivery Platform. While the vulnerability is in Service Delivery Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Service Delivery Platform accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-08-18	6.8	CVE-2026-60865
Oracle Corporation-- Service Delivery Platform	Vulnerability in the Service Delivery Platform product of Oracle Fusion Middleware (component: Messaging Enabler). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Service Delivery Platform. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Service Delivery Platform accessible data as well as unauthorized read access to a subset of Service Delivery Platform accessible data. CVSS 3.1 Base	2026-08-18	6.5	CVE-2026-60866

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).			
Otalio--Ship Property Management System	Unescaped stored values in application security page in Otalio Ship Property Management System versions before 2.22.0 allows authenticated attackers to escalate privileges via persistent cross-site scripting	2026-08-18	6.7	CVE-2025-9211
Pantherius--Modal Survey	Subscriber Insecure Direct Object References (IDOR) in Modal Survey <= 2.0.2.2.3 versions.	2026-08-18	4.3	CVE-2026-66634
Paolo--GeoDirectory	Contributor Cross Site Scripting (XSS) in GeoDirectory <= 2.8.172 versions.	2026-08-18	6.5	CVE-2026-68565
Papaki (Enartia S.A.)--Piraeus Bank WooCommerce Payment Gateway	Unauthenticated Broken Authentication in Piraeus Bank WooCommerce Payment Gateway 3.2.0 versions.	2026-08-18	6.5	CVE-2026-73398
Passionate Programmer Peter--WP Data Access	Unauthenticated Broken Access Control in WP Data Access <= 5.5.80 versions.	2026-08-20	5.9	CVE-2026-66595
Passter--Passter	The Passter WordPress plugin before 4.3.9 does not correctly match its own public endpoint paths when deciding which REST API requests may bypass global password protection, comparing them as an unanchored substring of the request URI rather than against the resolved route, allowing an unauthenticated attacker to read the content of globally password-protected posts and pages.	2026-08-21	5.3	CVE-2026-17559
patrickhener--goshs	goshs is a SimpleHTTPServer written in Go. Prior to version 2.1.0, `ShareHandler` reads the share token's `DownloadLimit` under `RLock`, releases the lock, serves the file, then re-acquires the lock to increment the counter. Concurrent requests all read the same `Downloaded`/`DownloadLimit` snapshot, all pass the check, and all are served - exceeding the operator's intended cap. Version 2.1.0 patches the issue.	2026-08-18	5.9	CVE-2026-50139
pkp--pkp-lib	A vulnerability was detected in pkp pkp-lib up to 3.3.0-22/3.4.0-10/3.5.0-4. The affected element is the function `_transformPHP` of the file classes/xslt/XSLTransformer.php. The manipulation results in xml external entity reference. The attack can be executed remotely. Upgrading to version 3.3.0-23, 3.4.0-11 and 3.5.0-5 is sufficient to fix this issue. The patch is identified as 78c699370ea43ae2784e1c4ace7c947d207f2b47. Upgrading the affected component is advised.	2026-08-19	4.7	CVE-2026-76572
ProfilePress--ProfilePress	The ProfilePress WordPress plugin before 4.17.1 does not strip shortcodes from two of its profile fields before rendering them on public pages, allowing unauthenticated attackers to store shortcodes that are then executed when the page is viewed, disclosing a chosen user's email address, login and registration date.	2026-08-21	6.5	CVE-2026-19848
projectcontour--contour	Contour is a Kubernetes ingress controller using Envoy proxy. In versions 1.23.0 through 1.33.4, when an `HTTPProxy` is configured with incompatible combination of both `.spec.virtualhost.tls.enableFallbackCertificate: true` and `.spec.virtualhost.jwtProviders`, Contour does not reject the configuration. Consequently, requests from clients that do not send TLS SNI or send an unrecognized SNI (one that does not match any `HTTPProxy` FQDN) bypass configured JWT verification and are proxied to upstream services without a valid token. This issue is fixed in Contour v1.33.5. Contour now rejects and marks invalid any `HTTPProxy` resources that combine `.spec.virtualhost.tls.enableFallbackCertificate: true` with `.spec.virtualhost.jwtProviders`. Affected resources will receive a status condition with the error reason `TLSIncompatibleFeatures`. As a workaround, do not enable	2026-08-19	6.5	CVE-2026-50149

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`spec.virtualhost.tls.enableFallbackCertificate` on `HTTPProxy` resources that also define `spec.virtualhost.jwtProviders`. Remove one of the two settings to avoid the invalid configuration.			
properfraction--kk Star Ratings Rate Post & Collect User Feedbacks	The The kk Star Ratings - Rate Post & Collect User Feedbacks plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 5.4.10.3. This is due to the software allowing users to execute an action that does not properly validate the 'payload' value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	2026-08-22	5.3	CVE-2026-3424
PublishPress-- PublishPress Series	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PublishPress PublishPress Series allows Stored XSS. This issue affects PublishPress Series: from n/a through 2.17.0.	2026-08-18	5.9	CVE-2026-27365
puemos--craftplan	Craftplan before 0.5.1 contains a broken access control vulnerability that allows unauthenticated attackers to read sensitive credentials by exploiting an unconditional authorization policy on the Settings resource. Attackers can send a GET request to the settings API endpoint with a valid record ID to retrieve decrypted SMTP passwords, email API keys, and email API secrets due to the read policy using an always-allow authorization check that bypasses all identity verification.	2026-08-21	5.9	CVE-2026-76876
pydio--cells	Pydio Cells 5.0.0 through 5.0.2 returns share-link details to any authenticated user. The REST handler for GET /a/share/link/{Uuid} in idm/share/rest/handler.go reads the workspace UUID from the path, calls LinkById, and writes the result with no authorization step, whereas the sibling handler for GET /a/share/cell/{Uuid} loads the workspace and requires MatchPolicies with ResourcePolicyAction_READ, returning a not-found error so that existence is not disclosed. Nothing compensates further down: GetLinkWorkspace reaches GetOrCreateWorkspace, which issues SearchWorkspace with a query carrying no ResourcePolicyQuery, and PrepareResourcePolicyQuery returns the query unmodified when that field is nil, so the workspace service applies no policy filter. The workspace UUID is not secret, because the unauthenticated public page served for a share link embeds it as START_REPOSITORY. Any account holding a standard user role can therefore submit the UUID and receive the link hash and URL, the owner's user identifier, the hidden share user login, the permission set, the download limit and count, the target users, the expiry, and the password-required flag, while a direct read of the shared node from the same account is refused.	2026-08-18	4.3	CVE-2026-76032
Pylons--webob	WebOb provides objects for HTTP requests and responses. Prior to 1.8.11, Response._make_location_absolute() in src/webob/response.py checks a Location value for a URI scheme or leading double slash before urllib.parse.urljoin() strips leading C0 control characters and spaces. An attacker-controlled value such as a space followed by a protocol-relative or absolute URL can therefore bypass SCHEME_RE and startswith("/") checks and be normalized to an off-host redirect. Request.relative_url() and webob.exc._HTTPMove subclasses, including HTTPFound, are also affected because they use the same unsafe URL joining behavior or bypass the earlier normalization path. An unauthenticated attacker who can influence an application's redirect target can send users to an attacker-controlled host for phishing or OAuth and SSO token theft, but exploitation requires the user to follow the redirect. This issue is fixed in version 1.8.11.	2026-08-20	6.1	CVE-2026-54770
RadiusTheme-- Homlisti	Subscriber Broken Access Control in Homlisti <= 3.1.2 versions.	2026-08-20	6.5	CVE-2026-66647
RARgames-- 4gaBoards	4gaBoards is a boards system for realtime project management. Prior to 3.3.9, 4gaBoards allows any authenticated user to enumerate account information for every user through GET /api/users and retrieve arbitrary accounts through GET /api/users/:id. The users/index and users/show actions rely only on the default is-authenticated policy in server/config/policies.js, and server/api/controllers/users/index.js returns the result of	2026-08-18	6.5	CVE-2026-53959

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sails.helpers.users.getMany() without requester-specific authorization or response sanitization. Responses expose email, phone, organization, name, isAdmin, ssoGoogleEmail, ssoGithubEmail, and other SSO-linked email fields, including data for administrators. This enables instance-wide user enumeration, privacy loss, and targeted phishing reconnaissance. This issue is fixed in version 3.3.9.			
Razorpay--Razorpay for WooCommerce	Unauthenticated Insecure Direct Object References (IDOR) in Razorpay for WooCommerce <= 4.8.7 versions.	2026-08-18	5.3	CVE-2026-74009
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in volsync-addon-controller. This vulnerability allows an attacker to inject malicious YAML (Yet Another Markup Language) code into the OpenShift Lifecycle Manager (OLM) Subscription resource. This is due to improper escaping of annotation values when they are rendered into YAML. Successful exploitation could lead to unauthorized modification or control over OLM Subscription configurations, potentially impacting software management within the cluster. This issue primarily affects systems where the 'volsync-addon-deploy-type: olm' annotation is explicitly enabled.	2026-08-19	6.2	CVE-2026-18874
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the Submariner operator. The Submariner Custom Resource (CR), used for configuring network connectivity, stores the IPsec pre-shared key (PSK) in an unencrypted format. This key, which is critical for securing communication between Kubernetes clusters, can be accessed by unauthorized parties. Such access enables an attacker to passively decrypt network traffic flowing between any two clusters in the mesh, resulting in sensitive information disclosure.	2026-08-18	6.5	CVE-2026-66781
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in search-indexer. This vulnerability allows a registered and authenticated managed cluster to tamper with or delete another cluster's indexed search data. This is possible because the delta-sync write paths in search-indexer do not properly restrict UPDATE/DELETE operations to data owned by the calling cluster. An attacker could exploit this by crafting specific user identifiers (UIDs) with a different cluster's prefix.	2026-08-19	6.8	CVE-2026-76827
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the must-gather component of Red Hat Advanced Cluster Management for Kubernetes. Certain ACM wrapper Custom Resources that embed Secret data are collected without redaction. When an administrator runs must-gather, credentials and tokens are captured in cleartext in the resulting archive, potentially exposing sensitive information to anyone with access to the archive.	2026-08-18	5.5	CVE-2026-73834
Red Hat--Red Hat Advanced Cluster Management for Kubernetes 2	A flaw was found in the must-gather component of Red Hat Advanced Cluster Management for Kubernetes. The cluster Proxy object is dumped in raw form, bypassing the oc inspect redaction that would normally sanitize sensitive fields. This exposes proxy basic-auth credentials in the must-gather archive, potentially disclosing sensitive authentication information to anyone with access to the archive.	2026-08-18	5.5	CVE-2026-75485
Red Hat--Red Hat Build of Keycloak	A flaw was found in the group policy provider of Keycloak authorization services, which is used to manage fine-grained access control to resources. The issue occurs when the system evaluates group-based policies using tokens that only contain group names rather than full paths. If two groups in different parts of the organization share the same name, a user in the unauthorized group can be mistaken for a member of the authorized group. This can allow a user to gain unauthorized access to protected resources they should not be able to reach.	2026-08-18	5.3	CVE-2026-19608
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the 'ipa-enrollment' SLAPI plugin. A remote authenticated client can exploit a null pointer dereference vulnerability by sending a malformed Lightweight Directory Access Protocol (LDAP) extended operation. By omitting the request value for the 'JOIN_OID' in the 'ipa-enrollment' extended operation, an attacker can trigger a server crash, potentially causing a denial of service.	2026-08-20	6.5	CVE-2026-73199

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in BlueZ. Insufficient validation of packet length fields in GetFolderItems responses within the Audio/Video Remote Control Profile (AVRCP) implementation allows a malicious Bluetooth device within range to cause an out-of-bounds memory read. This vulnerability, affecting the parse_media_element() and parse_media_folder() functions, can lead to a crash of the bluetoothd daemon, resulting in a Denial of Service (DoS). It could also potentially expose sensitive heap memory contents. Exploitation requires user interaction to pair with the malicious device.	2026-08-18	6.3	CVE-2026-75032
Red Hat--Red Hat Enterprise Linux 10	An out-of-bounds read vulnerability was found in swtpm's SWTPM_NVRAM_CheckHeader() function. The entry guard checks the buffer length against sizeof(bh), where bh is a pointer, instead of sizeof(*bh), the actual struct size. This allows an undersized buffer to pass validation, causing a 2-byte heap overread on 64-bit systems (6 bytes on 32-bit) when accessing the totlen field. This may cause daemon termination on some platforms and leaks heap data to the log.	2026-08-19	6.1	CVE-2026-75900
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in libsoup's SoupServer HTTP Range header processing. The sort_ranges() comparator in soup-message-headers.c truncates a 64-bit subtraction result to 32-bit int, flipping the sign for range offsets differing by more than INT_MAX. This causes silent omission of requested byte ranges from HTTP 206 Partial Content responses on resources larger than approximately 2 GB.	2026-08-20	5.3	CVE-2026-77014
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in FreeIPA. A low-privilege authenticated user can exploit this vulnerability by submitting an oversized One-Time Password (OTP) key value. This oversized key is then decoded and re-encoded without proper size limits, consuming excessive CPU and memory resources. This can lead to a denial of service, degrading the availability of the IPA service.	2026-08-20	4.3	CVE-2026-73196
Red Hat--Red Hat JBoss Enterprise Application Platform 7	A flaw was found in mod_cluster's AdvertiseListenerImpl (org.jboss.modcluster core module). A single crafted UDP multicast datagram with a valid HTTP status line and a "Server:" header but without the "Date:", "Digest:", and "Sequence:" headers triggers a NullPointerException in verifyDigest() that is not caught by the worker thread's exception handler. This causes the advertise listener thread to terminate permanently. The failure is silent (isListening() continues to return true) and persists until the node is restarted. The crash occurs before the AdvertiseSecurityKey comparison, so deployments with a configured security key are still affected.	2026-08-19	4.3	CVE-2026-76166
renovatebot--renovate	Renovate versions from 43.65.0 before 43.102.11 contain a remote code execution vulnerability in bazel-module and bazelisk managers when using lockFileMaintenance. Attackers can execute arbitrary code by providing malicious dependencies that are referenced in bazel mod deps calls, such as within ctx.execute statements.	2026-08-19	6.3	CVE-2026-76226
renovatebot--renovate	Renovate versions >=32.124.0 and before 42.68.5 (and Mend renovate-ce/renovate-ee before 13.3.0) contain a command injection vulnerability in Gradle Wrapper artifact handling. When Renovate processes Gradle Wrapper updates, it invokes a wrapper update command via a shell (e.g. /bin/sh -c/gradlew :wrapper --gradle-distribution-url <value>). If an attacker supplies a malicious gradle-wrapper.properties whose distributionUrl contains shell command substitution syntax such as \$(...), the shell evaluates it before Gradle parses the URL, resulting in arbitrary command execution in the Renovate runtime. Exploitation requires the attacker to introduce the malicious file into a repository that Renovate scans; the issue occurs even when allowScripts is disabled.	2026-08-19	6.7	CVE-2026-76228
renovatebot--renovate	Renovate versions from 39.218.0 before 40.33.0 contain an arbitrary command injection vulnerability in the kustomize manager where user-provided chart names are appended to helm pull commands without proper sanitization. Attackers with repository write access can craft malicious kustomization.yaml files with specially	2026-08-19	6.7	CVE-2026-76229

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	crafted chart names to execute arbitrary commands on the Renovate host machine.			
renovatebot--renovate	Renovate versions from 35.63.0 before 40.33.0 contain a command injection vulnerability in the npm manager where user-provided packageName values are appended to npm install commands without proper sanitization. Attackers with repository write access can craft malicious Renovate configuration files to execute arbitrary commands on the machine running Renovate.	2026-08-19	6.7	CVE-2026-76230
renovatebot--renovate	Renovate versions from 32.135.0 before 40.33.0 contain a command injection vulnerability in the hermit manager where user-provided dependency names are appended to install and uninstall commands without proper sanitization. Attackers with repository write access can provide maliciously named hermit dependencies to execute arbitrary commands on the machine running Renovate.	2026-08-19	6.7	CVE-2026-76231
renovatebot--renovate	Renovate versions from 31.51.0 before 40.33.0 contain a command injection vulnerability in the helmv3 manager where the repository parameter is appended to helm registry login commands without proper sanitization. Attackers with repository write access can craft malicious Chart.yaml files to execute arbitrary commands on the machine running Renovate.	2026-08-19	6.7	CVE-2026-76232
renovatebot--renovate	Renovate versions from 39.53.0 before 40.33.0 contain a command injection vulnerability in the gleam manager where the depName parameter is appended to gleam deps update commands without proper sanitization. Attackers with repository write access can craft malicious gleam.toml files to execute arbitrary commands on the machine running Renovate.	2026-08-19	6.7	CVE-2026-76233
renovatebot--renovate	Renovate versions from 42.68.1 before 42.96.3 (and from 42.68.1 before 43.4.4), including corresponding Docker images (renovate/renovate, mend/renovate-ce, renovate-ee-server, renovate-ee-worker >=13.3.0 <13.6.0), fail to restrict environment variables to an allowlist when spawning child processes. As a result, child processes (e.g. npm install, postUpgradeTasks, postUpdateOptions) gain full access to all environment variables of the Renovate process, allowing insider or outside attackers to exfiltrate secrets accessible to the Renovate deployment.	2026-08-19	5.5	CVE-2026-76227
rometheme--RomethemeForm For Elementor	Contributor Broken Access Control in RomethemeForm For Elementor <= 1.2.6 versions.	2026-08-18	4.3	CVE-2026-74003
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, the modoboa driver of the password plugin could leak a Modoboa API authentication token to a user-controlled host via crafted session data. This issue only affects Roundcube instances using the password plugin with its modoboa driver.	2026-08-17	6.4	CVE-2026-75010
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, the "Add to address book" action was subject to stored XSS.	2026-08-17	5.4	CVE-2026-74999
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, improper HTML/CSS sanitization of the SVG animate "by" attribute may lead to remote image blocking bypass, which in turn may lead to information disclosure or privilege escalation.	2026-08-17	5.8	CVE-2026-75000
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, an unclosed url() in a FuncIRI attribute of an SVG image could evade the remote image blocking, which may lead to information disclosure or privilege escalation.	2026-08-17	5.8	CVE-2026-75003
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, insufficient Cascading Style Sheets (CSS) sanitization in HTML e-mail messages may lead to SSRF or Information Disclosure, e.g., if stylesheet links point to local network hosts. This issue exists because of insufficient fixes for CVE-2026-35540, CVE-2026-48843 and CVE-2026-62643.	2026-08-17	5.8	CVE-2026-75006

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, the LDAP search filter was subject to injection via unescaped %u/%fu/%d substitution, which may lead to information disclosure or privilege escalation.	2026-08-17	5.4	CVE-2026-75007
Roundcube--Webmail	In Roundcube Webmail before 1.6.18 and 1.7.x before 1.7.3, improper rule name quoting could lead to managesieve_disabled_actions setting bypass via a crafted rule name in a Sieve script. This issue only affects Roundcube instances using the managesieve plugin.	2026-08-17	4.3	CVE-2026-75004
rubengc--AutomatorWP Automator plugin for no-code automations, webhooks & custom integrations in WordPress	The AutomatorWP - Automator plugin for no-code automations, webhooks & custom integrations in WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.8.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve all ConvertKit form data configured by the site's manager account, exposing integration details intended to be restricted to plugin managers. The required nonce is localized on every admin page load, making it accessible to any authenticated user who can reach /wp-admin.	2026-08-22	4.3	CVE-2026-76057
rubengc--AutomatorWP Automator plugin for no-code automations, webhooks & custom integrations in WordPress	The AutomatorWP - Automator plugin for no-code automations, webhooks & custom integrations in WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.8.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve the site's configured Campaign Monitor mailing list catalog, including all list IDs and names, that should be restricted to users with the plugin's manager capability. The required nonce is emitted unconditionally on every WordPress admin page via wp_localize_script, meaning any subscriber visiting /wp-admin/profile.php can obtain it without any elevated access.	2026-08-22	4.3	CVE-2026-76074
runtipi--runtipi	Runtipi is a personal homeserver orchestrator. In 4.10.0 and earlier, Runtipi accepts symbolic links from an attacker-controlled backup archive and copies them into live application paths during the backup restore flow. An authenticated attacker can plant user-config/app.env as a symlink to an arbitrary reachable path and then send PUT /api/user-config/demoapp3:_user with attacker-controlled appEnv content. FilesystemService.writeTextFile() follows the planted link, allowing content to be written outside the intended restore and user-config directory boundary with Runtipi process permissions. This issue is fixed in version 4.10.1.	2026-08-21	6.5	CVE-2026-55168
saleor--saleor	Saleor is an e-commerce platform. From 3.14.67 until 3.21.67, 3.22.63, and 3.23.22, a broken authorization check in saleor/permission/utils.py can incorrectly authorize unauthenticated GraphQL requests. The flaw permits anonymous callers to use the channelUpdate() mutation to change channel order settings such as allowUnpaidOrders even when the response reports PermissionDenied. The same permission utility can expose hidden objects through the pageType() and translation() queries, including attributes whose visibleInStorefront field is false and that should be visible only to users with management permissions. This issue is fixed in versions 3.21.67, 3.22.63, and 3.23.22.	2026-08-18	6.5	CVE-2026-48744
sambitraj--Student-Management-System	A vulnerability was detected in sambitraj Student-Management-System up to 56ba287f2e9031523ccb4244cb6e3fe530e4e5d5. Affected by this issue is some unknown functionality of the component Dashboard. The manipulation of the argument roll_no/teacher_name results in sql injection. The attack can be executed remotely. The exploit is now public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-23	6.3	CVE-2026-78056
sambitraj--Student-	A flaw has been found in sambitraj Student-Management-System up to 56ba287f2e9031523ccb4244cb6e3fe530e4e5d5. This affects an unknown part of the component Management Mutation Handler. This manipulation of the	2026-08-23	6.3	CVE-2026-78057

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management-System	argument roll_no/name/father_name/class/mobile/email/password/remark causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.			
sgoudelis--ground-station	Ground Station is a browser-based suite for satellite tracking, SDR reception, hardware control, and telemetry decoding. Prior to version 0.4.13, the unauthenticated configure-sdr Socket.IO command accepts a recordingPath for the sigmf-playback SDR and backend/handlers/entities/sdr.py stores it without validation before backend/hardware/sigmfprobe.py opens the path without enforcing containment. An absolute path or parent-directory escape ending in .sigmf-meta is parsed as JSON and returned in reply["data"]["metadata"] by the get-sdr-parameters flow. Exploitation requires the metadata file to be readable JSON and to have a sibling .sigmf-data file, but it can disclose contents outside backend/data/recordings without authentication. This issue is fixed in version 0.4.13.	2026-08-19	5.3	CVE-2026-53452
Shabti Kaplan--Frontend Admin by DynamiApps	Contributor Cross Site Scripting (XSS) in Frontend Admin by DynamiApps <= 3.29.10 versions.	2026-08-18	6.5	CVE-2026-66638
siteground--AI Agent by SiteGround	The AI Agent by SiteGround plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.2.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to upload images to the WordPress media library, bypassing the upload_files capability restriction that Contributors are normally subject to, as authenticated attackers with Contributor-level access or above can satisfy the endpoint's nonce and permission checks. The sg_ai_studio_gutenberg_nonce required by the endpoint is emitted to any user with block editor access - including Contributors - making the absent upload_files check the sole barrier to exploitation.	2026-08-20	5.3	CVE-2026-17153
siteground--Speed Optimizer The All-In-One Performance-Boosting Plugin	The Speed Optimizer - The All-In-One Performance-Boosting Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Image Tag Attributes in all versions up to, and including, 7.8.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when the site administrator has enabled the Lazy Load Media option in the plugin settings.	2026-08-19	6.4	CVE-2026-15421
siyuan-note--siyuan	SiYuan versions before v3.7.4 fail to validate that packageName matches the downloaded package content in bazaar install endpoints. Attackers with same-origin access can overwrite existing trusted plugins by supplying mismatched packageName and repoURL parameters, achieving persistence across application restarts.	2026-08-22	6.6	CVE-2026-62204
siyuan-note--siyuan	SiYuan before v3.8.0 interpolates secret placeholders into the destination URL parameter of the http_request MCP tool, allowing attackers to exfiltrate stored secrets. An MCP client can craft a request with an attacker-controlled URL containing secret placeholders to send plaintext secret values to any public host without confirmation.	2026-08-22	4.9	CVE-2026-59809
siyuan-note--siyuan	SiYuan versions before v3.8.0 contain an incomplete path blocklist in the MCP file tool that fails to restrict access to sensitive workspace files protected by the HTTP API. Authenticated administrators can read plaintext publish-mode passwords from data/.siyuan/publishAccess.json and access other sensitive files like data/templates and data/snippets/conf.json.	2026-08-22	4.9	CVE-2026-60083

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siyuan-note--siyuan	SiYuan versions before 3.7.4 contain a cross-site request forgery vulnerability in the session-cookie authentication branch of CheckAuth() that lacks Origin/Referer validation and sets no explicit SameSite attribute on session cookies. Attackers can craft malicious web pages that perform unauthorized actions on behalf of authenticated users by submitting requests with valid session cookies, relying on browser default SameSite policies rather than server-enforced protections.	2026-08-17	4.2	CVE-2026-74867
siyuan-note--siyuan	SiYuan before v3.7.4 contains an insufficient access control vulnerability in the /api/lute/spinBlockDOM endpoint, which is guarded only by CheckAuth middleware instead of CheckAdminRole like its sibling endpoint. Authenticated users with RoleEditor or RoleReader roles can invoke the endpoint to transform arbitrary DOM input, and large payloads cause endpoint starvation through per-path mutex serialization.	2026-08-18	4.3	CVE-2026-74903
sonos--tract	A security vulnerability has been detected in sonos tract up to 0.23.4. This impacts the function Tensor::from_raw_dt_align of the file data/src/tensor.rs of the component ONNX Initializer Loader. Such manipulation leads to incorrect calculation of buffer size. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The name of the patch is 66b10bda8895f4bfa8c205361f0125cdf51f99b. It is best practice to apply a patch to resolve this issue.	2026-08-18	4.3	CVE-2026-75093
SourceCodester--Best Employee Management System	A security vulnerability has been detected in SourceCodester Best Employee Management System 1.0. This affects an unknown function of the file /assets/uploadImage/Profile/. Such manipulation leads to exposure of information through directory listing. It is possible to launch the attack remotely.	2026-08-17	5.3	CVE-2026-19987
SourceCodester--CET Automated Grading System with AI Predictive Analytics	A vulnerability was detected in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. This affects the function add_grade of the file /index.php. Performing a manipulation of the argument student_id results in improper authorization. The attack can be initiated remotely.	2026-08-20	6.3	CVE-2026-76999
SourceCodester--Class and Exam Timetabling System	A vulnerability has been found in SourceCodester Class and Exam Timetabling System 1.0. Affected is an unknown function of the file /admin/edit_user_account.php of the component User Account Update. Such manipulation of the argument id/username leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-08-23	5.4	CVE-2026-78115
SourceCodester--Class and Exam Timetabling System	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. Affected by this issue is some unknown functionality of the file /BSCE2.php. Such manipulation of the argument course leads to cross site scripting. The attack may be launched remotely. The exploit is publicly available and might be used.	2026-08-17	4.3	CVE-2026-75077
SourceCodester--Class and Exam Timetabling System	A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0. This affects an unknown part of the file /BSHRM1.php. Performing a manipulation of the argument course results in cross site scripting. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	2026-08-17	4.3	CVE-2026-75078
SourceCodester--Class and Exam Timetabling System	A weakness has been identified in SourceCodester Class and Exam Timetabling System 1.0. Affected is an unknown function of the file /BSIS1.php. Executing a manipulation of the argument course can lead to cross site scripting. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-23	4.3	CVE-2026-78054
SourceCodester--Class and Exam	A security vulnerability has been detected in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /BSIT2.php. The manipulation of the argument course leads to cross site	2026-08-23	4.3	CVE-2026-78055

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Timetabling System	scripting. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.			
SourceCodester--Dynamic Input Field Generator Using HTML, CSS, and PHP	A weakness has been identified in SourceCodester Dynamic Input Field Generator Using HTML, CSS, and PHP 1.0. This impacts the function saveUser of the file /public/submit.php. This manipulation of the argument Researcher causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-21	6.3	CVE-2026-77392
SourceCodester--Dynamic Input Field Generator Using HTML, CSS, and PHP	A security flaw has been discovered in SourceCodester Dynamic Input Field Generator Using HTML, CSS, and PHP 1.0. This affects an unknown function. The manipulation results in cross-site request forgery. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-08-21	4.3	CVE-2026-77391
SourceCodester--Online Examination & Learning Management System	A vulnerability has been found in SourceCodester Online Examination & Learning Management System 1.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. The attack can be initiated remotely.	2026-08-18	4.3	CVE-2026-75151
SourceCodester--Simple Online Food Ordering System	A weakness has been identified in SourceCodester Simple Online Food Ordering System 1.0. The affected element is an unknown function of the file /admin/ajax.php?action=save_category. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-20	6.3	CVE-2026-76997
SourceCodester--Simple Online Food Ordering System	A vulnerability was identified in SourceCodester Simple Online Food Ordering System 1.0. This issue affects some unknown processing of the file /admin/ajax.php?action=save_menu. The manipulation of the argument img leads to unrestricted upload. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2026-08-20	4.7	CVE-2026-76995
SourceCodester--Stock Management System	A vulnerability has been found in SourceCodester Stock Management System 1.0. This vulnerability affects unknown code of the file /php_action/printOrder.php. Such manipulation of the argument clientName/clientContact leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2026-08-23	4.3	CVE-2026-78059
SourceCodester--Stock Management System	A vulnerability was found in SourceCodester Stock Management System 1.0. This issue affects some unknown processing of the file /php_action/getOrderReport.php. Performing a manipulation of the argument clientName/clientContact results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	2026-08-23	4.3	CVE-2026-78060
Splunk--AD LDAP app for Splunk SOAR	In versions below 2.3.8 of the AD LDAP app for Splunk SOAR, a user who holds a role with permission to run actions could inject crafted input into an Active Directory query to enumerate Active Directory objects, including accounts, groups, and organizational units, read sensitive attributes from arbitrary directory objects, and redirect account modification actions to unintended objects. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	5.4	CVE-2026-76373
Splunk--AD LDAP app for Splunk SOAR	In versions below 2.3.8 of the AD LDAP app for Splunk SOAR, a user who holds a role with permission to run actions could expose sensitive credentials by invoking an action that causes the full connector process environment to be written to a persistent debug log file in plaintext. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-	2026-08-19	5	CVE-2026-76375

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).			
Splunk--AD LDAP app for Splunk SOAR	In versions below 2.3.8 of the AD LDAP app for Splunk SOAR, a user who holds a role with permission to run actions could cause sensitive Active Directory response data to be written to a persistent debug log file by triggering write operations through the app. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76374
Splunk--AWS IAM app for Splunk SOAR	In versions below 2.1.9 of the AWS IAM app for Splunk SOAR, a user who holds a role with permission to run actions could expose sensitive AWS credentials by invoking an action that accepts the credentials parameter, because the parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76376
Splunk--Azure AD Graph app for Splunk SOAR	In versions below 2.5.3 of the Azure AD Graph app for Splunk SOAR, a user who holds a role with permission to run actions could expose a sensitive password by invoking the reset password action, because the action's temp_password parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76377
Splunk--Cisco Secure Malware Analytics app for Splunk SOAR	In versions below 2.4.5 of the Cisco Secure Malware Analytics app for Splunk SOAR, a user who holds a role with permission to run actions could expose a sensitive sample password by invoking the detonate file action, because the action's sample_password parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76378
Splunk--Cisco Talos Intelligence for Enterprise Security Cloud	In Cisco Talos Intelligence for Enterprise Security Cloud versions below 1.0.3, an unauthenticated user could access the add-on OpenAPI specification through Splunk Web static file paths. The exposed specification could allow for reconnaissance of the add-on Representational State Transfer (REST) API endpoints and authentication model. The vulnerability is possible because the generated OpenAPI specification is packaged in a static file path that Splunk Web serves without authentication. For more information see Deploy Cisco Talos Intelligence for Splunk Enterprise Security (https://help.splunk.com/en/splunk-enterprise-security-8/user-guide/8.0/introduction/deploy-cisco-talos-intelligence-for-splunk-enterprise-security-cloud-only) in the Splunk documentation.	2026-08-19	5.3	CVE-2026-76390
Splunk--Cisco Webex app for Splunk SOAR	In versions below 2.2.1 of the Cisco Webex app for Splunk SOAR, a user who holds a role with permission to run actions could expose a sensitive meeting password by invoking the schedule meeting action, because the action's password parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76379

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).			
Splunk--CrowdStrike OAuth API app for Splunk SOAR	In versions below 5.1.3 of the CrowdStrike OAuth API app for Splunk SOAR, a user who holds a role with permission to run actions could expose a sensitive document password by invoking either the detonate file or detonate url action, because the action's document_password parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76380
Splunk--MS Graph for Active Directory app for Splunk SOAR	In versions below 1.5.2 of the MS Graph for Active Directory app for Splunk SOAR, a user who holds a role with permission to run actions could expose a sensitive password by invoking the reset password action, because the action's temp_password parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76381
Splunk--Nmap Scanner	In Nmap Scanner versions below 3.0.15, a user who holds a role that can edit, create, or run playbooks in Splunk SOAR could run the scan network action in a Safe Mode playbook while that action is listed as read-only, which could allow for command execution or other changes on a target system through Nmap Scripting Engine scripts. The vulnerability is possible because the Nmap Scanner connector action manifest classifies the scan network action as read-only even though the action accepts script parameters that can perform write operations. For more information see Manage settings for a playbook in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-cloud/build-playbooks/manage-playbooks-and-playbook-settings/manage-settings-for-a-playbook-in-splunk-soar-cloud) in the Splunk documentation.	2026-08-19	6.6	CVE-2026-76372
Splunk--Phantom app for Splunk SOAR	In versions below 3.8.5 of the Phantom app for Splunk SOAR, a user who holds a role with permission to run actions could expose a sensitive archive password by invoking the deflate item action, because the action's password parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76382
Splunk--RSA SecurID Authentication Manager app for Splunk SOAR	In versions below 1.0.5 of the RSA SecurID Authentication Manager app for Splunk SOAR, a user who holds a role with permission to run actions could expose a sensitive token serial by invoking either the enable token or revoke token action, because the action's token_serial parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76383
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.0, a user who does not hold the "admin" or "power" Splunk roles could obtain predictable or default credentials for connected container services. The use of hard-coded credentials is possible because Splunk AI	2026-08-19	5.4	CVE-2026-76392

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Toolkit generates or stores credentials for connected container services using predictable or hard-coded default values. For more information see Connections tab in the AI Toolkit (https://help.splunk.com/en/splunk-cloud-platform/apply-machine-learning/use-ai-toolkit/5.7.2/ai-toolkit-commands-macros-and-visualizations/connections-tab-in-the-ai-toolkit) in the Splunk documentation.			
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.0, a user who can upload models could overwrite a model being uploaded by another user by sending a concurrent upload request for the same model name, causing the resulting model lookup entry to reference attacker-controlled content. The race condition is possible because Splunk AI Toolkit does not verify that the uploaded content belongs to the request that creates the model lookup entry. For more information see Troubleshoot the Splunk Machine Learning Toolkit (https://help.splunk.com/en/splunk-cloud-platform/apply-machine-learning/machine-learning-toolkit-user-guide/5.5.0/troubleshooting-mltk/troubleshoot-the-splunk-machine-learning-toolkit) in the Splunk documentation.	2026-08-19	5.9	CVE-2026-76393
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 6.0.1, a user who does not hold the "admin" or "power" Splunk roles could delete the experiment history of another user without permission through the Representational State Transfer (REST) API. The vulnerability is possible because Splunk AI Toolkit deletes experiment history before it verifies that the user can delete the associated experiment. For more information see Experiment Assistants (https://help.splunk.com/en/splunk-cloud-platform/apply-machine-learning/use-ai-toolkit/5.6.4/experiment-assistants) in the Splunk documentation.	2026-08-19	4.3	CVE-2026-76398
Splunk--Splunk Attack Analyzer Connector for Splunk SOAR	In versions below 2.2.1 of the Splunk Attack Analyzer Connector for Splunk SOAR, a user who holds a role with permission to run actions could expose a sensitive archive password by invoking either the detonate file or detonate url action, because the action's archive_password parameter is not masked and is shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameter as a password. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76384
Splunk--Splunk Connect for Kafka	In Splunk Connect for Kafka versions below 2.2.7, an unauthenticated user who can reach the Kafka Connect Representational State Transfer (REST) API and influence responses from a Hypertext Transfer Protocol (HTTP) Event Collector endpoint in Splunk Enterprise could cause the connector to retry failed event batches until event delivery stops. The vulnerability is possible because HTTP Event Collector delivery retry handling uses an unbounded default for failed batches instead of a finite retry limit. For more information see Install Splunk Connect for Kafka (https://help.splunk.com/en/data-management/integrate-data-with-add-ons/splunk-connect-for-kafka/2.2/install/install-splunk-connect-for-kafka), Data ingestion parameters for Splunk Connect for Kafka (https://help.splunk.com/en/data-management/integrate-data-with-add-ons/splunk-connect-for-kafka/2.2/overview/data-ingestion-parameters-for-splunk-connect-for-kafka), and Set up and use HTTP Event Collector with configuration files (https://help.splunk.com/en/splunk-enterprise/get-data-in/get-started-with-getting-data-in/9.4/get-data-with-http-event-collector/set-up-and-use-http-event-collector-with-configuration-files) in the Splunk documentation.	2026-08-19	5.9	CVE-2026-76400
Splunk--Splunk Connect for Kafka	In Splunk Connect for Kafka versions below 2.2.7, an unauthenticated user who can reach the Kafka Connect Representational State Transfer (REST) API could configure timestamp extraction with a crafted regular expression and matching event data to block a Kafka Connect worker thread, stopping event delivery for the affected connector. The vulnerability is possible because timestamp extraction evaluates customer-supplied regular expressions without a time limit. For more information see Install Splunk Connect for Kafka (<a #"="" href="https://help.splunk.com/en/data-</td><td>2026-08-19</td><td>5.9</td><td>CVE-2026-76401			

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	management/integrate-data-with-add-ons/splunk-connect-for-kafka/2.2/install/install-splunk-connect-for-kafka) and Data ingestion parameters for Splunk Connect for Kafka (https://help.splunk.com/en/data-management/integrate-data-with-add-ons/splunk-connect-for-kafka/2.2/overview/data-ingestion-parameters-for-splunk-connect-for-kafka) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.13, an unauthenticated user who tricks another user into visiting a malicious web page could run unauthorized JavaScript in that user's browser. This could allow for unauthorized access to all relevant data available to that user and actions that affect system integrity. The Cross-Site Scripting (XSS) is possible because Splunk Web does not validate the origin and source of messages received by a page message handler. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The unauthenticated user should not be able to exploit the vulnerability at will.	2026-08-19	6.8	CVE-2026-76252
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.1, 10.2.6, 10.0.8, and 9.4.13, a user who does not hold the "admin" or "power" Splunk roles could trick another user into running arbitrary Search Processing Language (SPL) commands through the Data Model Editor using the permissions of the affected user. The commands could access all relevant data available to the affected user and affect system integrity. The vulnerability is possible because Splunk Web does not apply SPL safeguards for risky commands when the Data Model Editor runs the base search for auto-extracted fields. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who does not hold the "admin" or "power" Splunk roles should not be able to exploit the vulnerability at will. For more information see SPL safeguards for risky commands (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/best-practices-for-splunk-platform-security/spl-safeguards-for-risky-commands) and Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	6.4	CVE-2026-76255
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, and Splunk Secure Gateway versions below 3.10.10, 3.9.24, and 3.8.71, a user who holds a Splunk role with permissions to list storage passwords but does not hold Splunk Secure Gateway administration privileges could access Mobile Device Management signing secrets that compromise all affected mobile-device enrollment trust through Splunk Secure Gateway. The vulnerability is possible because Splunk Secure Gateway Representational State Transfer (REST) API endpoints for deployment bundle, Security Assertion Markup Language setup, and companion app workflows do not require Splunk Secure Gateway administration privileges before processing requests.	2026-08-19	6.5	CVE-2026-76257
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, and Splunk Secure Gateway versions below 3.10.10, 3.9.24, and 3.8.71, a user who does not hold the "admin" or "power" Splunk roles could register an arbitrary companion app and cause Splunk Secure Gateway to forward mobile user requests, including tokens that compromise all relevant data available to the affected mobile user, to an attacker-controlled Uniform Resource Locator (URL). The vulnerability is possible because a hard-coded cryptographic key in the Splunk Secure Gateway companion app registration handler allows for arbitrary callback URL registration without restriction. For more information see Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	6.5	CVE-2026-76258

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user that holds a role with the <code>rest_properties_get</code> capability could read encrypted stored credentials through the Representational State Transfer (REST) API. Successful exploitation can expose relevant data protected by the stored credentials. The incorrect permission assignment is possible because the properties REST endpoint requires the <code>rest_properties_get</code> capability instead of the <code>list_storage_passwords</code> capability to read stored credentials. For more information see Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	6.5	CVE-2026-76260
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "user" Splunk role could craft a Dashboard Studio dashboard that runs attacker-controlled Search Processing Language (SPL) for another authenticated user. The attacker-controlled SPL could access all relevant data and affect system integrity and availability. The vulnerability is possible because Dashboard Studio does not consistently enforce the expected app-visibility authorization boundary before dashboard search query options reach search dispatch. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who holds the "user" Splunk role should not be able to exploit the vulnerability at will. For more information see Create search-based visualizations with <code>ds.search</code> (https://help.splunk.com/en/splunk-enterprise/create-dashboards-and-reports/dashboard-studio/10.4/use-data-sources/create-search-based-visualizations-with-ds.search) in the Splunk documentation.	2026-08-19	6.7	CVE-2026-76322
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could bypass Search Processing Language (SPL) safeguards for risky commands through the Job Details dashboard. The injected SPL could run using the permissions of an authenticated user who opens a crafted Job Details dashboard link. This could allow access to all relevant data and affect system integrity within those permissions. The vulnerability is possible because the Job Details dashboard does not correctly neutralize a caller-supplied search identifier before placing it into SPL searches. The vulnerability requires the attacker to phish the user by tricking them into opening the crafted link. The user who does not hold the "admin" or "power" Splunk roles should not be able to exploit the vulnerability at will. For more information see About jobs and job management (https://help.splunk.com/en/splunk-enterprise/search/search-manual/10.4/manage-jobs/about-jobs-and-job-management) in the Splunk documentation.	2026-08-19	6.4	CVE-2026-76323
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, and Splunk Secure Gateway versions below 3.10.9, 3.9.23, and 3.8.70, an unauthenticated user could trick a user who holds the "admin" or "sc_admin" Splunk roles into opening a crafted Splunk Web Uniform Resource Locator (URL). The resulting dashboard searches could run arbitrary Search Processing Language (SPL) commands with the permissions available to the affected user. The commands could expose all relevant data available to that user and affect search results or lookup data. The vulnerability is possible because Splunk Secure Gateway dashboards do not correctly neutralize caller-supplied values before using them in dashboard searches. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The unauthenticated user should not be able to exploit the vulnerability at will.	2026-08-19	6.4	CVE-2026-76327
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.1, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "power" Splunk role could store attacker-controlled Search Processing Language (SPL) in a dashboard. When another authenticated user exports the dashboard as a Portable Document Format (PDF) file, Splunk Enterprise runs the injected SPL using the permissions of that user. The injected SPL could access or	2026-08-19	6.7	CVE-2026-76328

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	modify data available to that user. The vulnerability is possible because Splunk Web does not sufficiently validate dashboard content before processing PDF exports. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who holds the "power" Splunk role should not be able to exploit the vulnerability at will. For more information see Generate PDFs of your reports and dashboards (https://help.splunk.com/en/splunk-enterprise/create-dashboards-and-reports/reporting-manual/9.4/report-management/generate-pdfs-of-your-reports-and-dashboards) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user could trick a user who holds the "admin" Splunk role into opening a crafted link to Monitoring Console. When that user opens the link, Splunk Enterprise runs attacker-controlled Search Processing Language (SPL) using the permissions of that user. The injected SPL could expose data available to that user or modify lookup data. The vulnerability is possible because Monitoring Console does not sufficiently validate data used to build dashboard searches. The vulnerability requires the attacker to phish the user by tricking them into opening the crafted link. The unauthenticated user should not be able to exploit the vulnerability at will.	2026-08-19	6.4	CVE-2026-76329
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "power" Splunk role could store a Dashboard Studio workflow action containing attacker-controlled Search Processing Language (SPL). When another authenticated user selects the action from Event Actions and selects Continue, Splunk Enterprise runs the injected SPL using the permissions of that user. The injected SPL could access or modify data available to that user. The vulnerability is possible because Dashboard Studio does not sufficiently validate workflow-action URLs before submitting requests. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who holds the "power" Splunk role should not be able to exploit the vulnerability at will.	2026-08-19	6.4	CVE-2026-76334
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could execute attacker-chosen Structured Query Language (SQL) queries through the Data Orchestration jobs endpoint, allowing for access to substantially all data stored by Data Orchestration, including jobs owned by other users and stored connection credentials. The vulnerability is possible because Data Orchestration builds a database query from user-controlled job filter values without using parameterized queries. For more information see About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access) in the Splunk documentation.	2026-08-19	6.5	CVE-2026-76343
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, a user with a high-privilege Splunk role that can manage search head clustering could use the search head cluster member bundle Representational State Transfer (REST) API to write files to locations that the user account running Splunk Enterprise can write to, which could allow for remote code execution. Successful exploitation could result in access to all relevant data and could affect the integrity and availability of the Splunk deployment. The vulnerability does not affect Splunk Enterprise versions below 10.4. The vulnerability is possible because the search head cluster member bundle REST API does not enforce the expected authorization boundary and does not validate bundle paths before accepting bundle content. For more information see Using the REST API reference (https://help.splunk.com/en/splunk-enterprise/rest-api-reference/10.2/introduction/using-the-rest-api-reference), About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access), and About distributed	2026-08-19	6	CVE-2026-76345

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	search (https://help.splunk.com/en/splunk-enterprise/administer/distributed-search/9.4/overview-of-distributed-search/about-distributed-search) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user could trick an authenticated user into running arbitrary Search Processing Language (SPL) commands using the permissions of the authenticated user through a crafted Splunk Web link. The SPL commands could access all relevant data. The vulnerability does not affect Splunk Enterprise 10.4 versions and above. The vulnerability is possible because Splunk Web substitutes form token values supplied through the Uniform Resource Locator (URL) into SPL searches without neutralizing them. The vulnerability requires the attacker to phish the user by tricking them into opening the crafted link. The unauthenticated user should not be able to exploit the vulnerability at will. For more information see Token reference (https://help.splunk.com/en/splunk-enterprise/create-dashboards-and-reports/simple-xml-dashboards/10.2/simple-xml-reference/token-reference) in the Splunk documentation.	2026-08-19	6.4	CVE-2026-76349
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, and Splunk Secure Gateway versions below 3.10.9, 3.9.23, and 3.8.70, a user who does not hold the "admin" or "power" Splunk roles could read Spacebridge asymmetric private keys, which are secrets that compromise affected Spacebridge private-key material stored in the app collection, through the Splunk Secure Gateway App Key Value Store Representational State Transfer (REST) API. The vulnerability is possible on instances upgraded from older Splunk Secure Gateway deployments when the private-key migration remains incomplete, leaving key material in a collection with an insecure default access control list.	2026-08-19	5.3	CVE-2026-76261
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2 and 10.2.6, a user who does not hold the "admin" or "power" Splunk roles could delete Splunk Processing Language version 2 (SPL2) modules belonging to other users through the data management orchestrator interface. The vulnerability does not affect Splunk Enterprise versions below 10.2. The broken object level authorization is possible because the data management orchestrator does not verify that the requesting user owns the target resources before it deletes the modules. For more information see Manage SPL2-based apps (https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/10.4/meet-splunk-apps/manage-spl2-based-apps) in the Splunk documentation.	2026-08-19	5.4	CVE-2026-76263
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user that holds a role with the schedule_search capability could store a malicious script in an alert trigger condition field. When another user opens the crafted link, the script runs in the browser of that user and could access all data available to that user. The vulnerability is possible because Splunk Web uses the alert threshold value in generated alert trigger condition markup without escaping special characters. Successful exploitation requires another user to open the crafted link. For more information see Configure alert trigger conditions (https://help.splunk.com/en/splunk-enterprise/alert-and-respond/alerting-manual/10.4/manage-alert-trigger-conditions-and-throttling/configure-alert-trigger-conditions) and Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	5.7	CVE-2026-76318
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user could cause an authenticated user to run arbitrary Search Processing Language (SPL) searches on their behalf through the Event Type Builder. This could expose all relevant data and stored credentials. The vulnerability is possible when the Event Type Builder accepts cross-site request input and retains SPL-affecting values while building sample event searches. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a	2026-08-19	5.9	CVE-2026-76320

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	request within their browser. The unauthenticated user should not be able to exploit the vulnerability at will. For more information see Automatically find and build event types (https://help.splunk.com/en/splunk-enterprise/manage-knowledge-objects/knowledge-management-manual/9.0/event-types/automatically-find-and-build-event-types) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "power" Splunk role could create a malicious Splunk Web tour and cause arbitrary JavaScript to run in the browser of another user when that user opens a crafted tour link. The JavaScript runs in the browser of the affected user, allowing for access to all relevant data available to that user. The Cross-Site Scripting (XSS) vulnerability is possible because Splunk Web renders tour content and tour navigation links without sufficient output encoding and accepts a tour selector value that can be treated as markup. The vulnerability requires another user to open a crafted tour link. The user who holds the "power" Splunk role should not be able to trigger JavaScript execution in another user's browser without that user interaction.	2026-08-19	5.7	CVE-2026-76324
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could store a dashboard view that runs JavaScript in the browser of another user who opens it and hovers over a sparkline table cell, allowing for access to all relevant data and system integrity available to that user. The vulnerability is possible because the dashboard table renderer does not sufficiently restrict tooltip options or escape tooltip content before display.	2026-08-19	5.7	CVE-2026-76326
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, an unauthenticated user could read JavaScript files outside the Splunk Web static directory. The vulnerability is possible because Splunk Web does not restrict static file requests to the configured static directory.	2026-08-19	5.3	CVE-2026-76337
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could inject arbitrary Search Processing Language (SPL) commands through the geostats command. The injected SPL runs with the permissions of another authenticated user after that user initiates the attacker-controlled geostats search in Splunk Web. The injected SPL could expose all relevant data available to the second user, including stored credentials, and modify lookup files that the second user has permission to change. The vulnerability is possible because the geostats command does not sufficiently validate input before Splunk Enterprise processes it. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who does not hold the "admin" or "power" Splunk roles should not be able to exploit the vulnerability at will. For more information see geostats (https://help.splunk.com/en/splunk-enterprise/spl-search-reference/10.0/search-commands/geostats) in the Splunk documentation.	2026-08-19	5.4	CVE-2026-76339
Splunk--Splunk Enterprise	In Splunk Enterprise 10.4 versions below 10.4.2, an unauthenticated user could cause Splunk Enterprise to reload token-signing keys through the Representational State Transfer (REST) API. The vulnerability does not affect Splunk Enterprise versions below 10.4. The vulnerability is possible because the REST API does not require authentication or the change_authentication capability for the token-key reload action. For more information see Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	5.3	CVE-2026-76340
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "power" Splunk role could store attacker-controlled Search Processing Language (SPL) in a Table Editor dataset and share the dataset. A user who holds the "admin" Splunk role triggers the SPL when that user opens the dataset in the Table Editor. The SPL runs using the permissions of the second user and could	2026-08-19	5.4	CVE-2026-76341

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	expose all relevant data and modify limited data on the search head. The vulnerability is possible because the Table Editor does not apply SPL safeguards for risky commands when it prepares the dataset initial data. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who holds the "power" Splunk role should not be able to exploit the vulnerability at will. For more information see Define initial data for a new table dataset (https://help.splunk.com/en/splunk-enterprise/manage-knowledge-objects/knowledge-management-manual/9.4/create-and-edit-table-datasets/define-initial-data-for-a-new-table-dataset), SPL safeguards for risky commands (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/best-practices-for-splunk-platform-security/spl-safeguards-for-risky-commands), and Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.4/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.			
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "power" Splunk role could store risky Search Processing Language (SPL) commands in a Table Editor dataset and share the dataset. A user who holds the "admin" Splunk role triggers the commands when that user opens the dataset in the Table Editor. The commands run using the permissions of the second user and could expose all relevant data and modify lookup files. The vulnerability is possible because the Table Editor does not apply SPL safeguards for risky commands to the field-summary search that it runs for the Initial Data step. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who holds the "power" Splunk role should not be able to exploit the vulnerability at will. For more information see SPL safeguards for risky commands (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/best-practices-for-splunk-platform-security/spl-safeguards-for-risky-commands) and Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities) in the Splunk documentation.	2026-08-19	5.4	CVE-2026-76342
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds the "power" Splunk role could store a malicious script in dashboard sparkline format options and execute unauthorized JavaScript in the browser of another user who views the dashboard. If the other user holds the "admin" Splunk role, the script could access all relevant data available through Splunk Web and perform actions with that user's permissions. The vulnerability is possible because Splunk Web does not limit the permitted dashboard visualization options to safe presentation settings and does not escape tooltip values before rendering them. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who holds the "power" Splunk role should not be able to exploit the vulnerability at will. For more information see About configuring role-based user access (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/about-configuring-role-based-user-access) in the Splunk documentation.	2026-08-19	5.4	CVE-2026-76346
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, and Splunk Secure Gateway versions below 3.10.9, 3.9.23, and 3.8.70, a user who does not hold the "admin" or "power" Splunk roles could use Server-Side Request Forgery (SSRF) in report notifications to send system-authenticated requests to internal Splunk services, which could allow for changes to Search Head Cluster state and a denial of service. The vulnerability is possible because Splunk Secure Gateway does not validate report notification path values before it sends internal requests.	2026-08-19	5.4	CVE-2026-76347

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who does not hold the "admin" or "power" Splunk roles could submit a crafted knowledge bundle delta to delete arbitrary files accessible to Splunk Enterprise on a cluster manager. This could affect system integrity and disrupt service. The vulnerability is possible because knowledge bundle delta processing does not restrict removal paths to the staging directory and the endpoint does not enforce the expected authorization boundary. For more information see Knowledge bundle replication overview (https://help.splunk.com/en/splunk-enterprise/administer/distributed-search/10.4/knowledge-bundle-replication/knowledge-bundle-replication-overview) in the Splunk documentation.	2026-08-19	5.4	CVE-2026-76353
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, and Splunk Secure Gateway versions below 3.10.9, 3.9.23, and 3.8.70, a user who does not hold the "admin" or "power" Splunk roles could read sensitive Security Assertion Markup Language setup and instance settings information through Splunk Secure Gateway Representational State Transfer (REST) API endpoints. The vulnerability is possible because the affected Security Assertion Markup Language setup and instance settings REST API endpoints do not enforce authorization requirements before returning configuration information.	2026-08-19	4.3	CVE-2026-76256
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a low-privileged user that does not hold the "admin" or "power" Splunk roles could inject Structured Query Language (SQL) through the Representational State Transfer (REST) API, causing Splunk Enterprise to evaluate attacker-controlled text as part of a database query. The SQL injection is possible because the REST API incorporates user-supplied filter values into database queries without proper neutralization.	2026-08-19	4.3	CVE-2026-76309
Splunk--Splunk On-Call (VictorOps)	In Splunk On-Call (VictorOps) app versions below 1.0.43 on Splunkbase, a user who does not hold the "admin" or "power" Splunk roles could read a partially masked Application Programming Interface (API) key from the App Key Value Store (KV Store). The exposure is possible because the Splunk On-Call (VictorOps) app does not fully mask the API key before storing it in a KV Store collection that the user can read. For more information see About the app key value store (https://help.splunk.com/en/data-management/splunk-enterprise-admin-manual/9.2/administer-the-app-key-value-store/about-the-app-key-value-store) in the Splunk documentation.	2026-08-19	4.3	CVE-2026-76405
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user with app-install privileges could use path traversal during app installation to write files outside the intended temporary directory. The vulnerability is a path traversal in the archive extraction routine, which does not validate that extracted file paths stay within the intended destination directory. For more information see Manage roles and permissions in Splunk SOAR (On-premises) (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/manage-your-splunk-soar-on-premises-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-on-premises) and Add and configure apps and assets to provide actions in Splunk SOAR (On-premises) (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/manage-your-splunk-soar-on-premises-apps-and-assets/add-and-configure-apps-and-assets-to-provide-actions-in-splunk-soar-on-premises) in the Splunk documentation.	2026-08-19	6.5	CVE-2026-76358
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user who holds the Administrator role could use path traversal in the Universal Forwarder installer's archive extraction to write files outside the intended installation directory. The vulnerability is possible because the Universal Forwarder credentials-package extraction workflow does not verify that each archive member remains within the intended destination before extraction. For more information see Manage roles and permissions in Splunk SOAR (On-premises) (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/manage-your-splunk-soar-on-premises-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-on-premises) and Configure forwarders to send SOAR data to your Splunk deployment	2026-08-19	6.5	CVE-2026-76359

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/configure-administration-settings-in-splunk-soar-on-premises/configure-forwarders-to-send-soar-data-to-your-splunk-deployment) in the Splunk documentation.			
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user who holds the "Automation Engineer" role could run arbitrary Structured Query Language (SQL) statements against the Splunk SOAR database and create, read, update, or delete all data in the database. The vulnerability is possible because Splunk SOAR playbook automation data APIs incorporate user-supplied input into database queries without proper neutralization. For more information see Manage roles and permissions in Splunk SOAR Cloud (https://help.splunk.com/en/splunk-soar/soar-cloud/administer-soar-cloud/manage-your-splunk-soar-cloud-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-cloud) in the Splunk documentation.	2026-08-19	6.5	CVE-2026-76363
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user who holds the "Automation Engineer" Splunk SOAR role could run arbitrary Structured Query Language (SQL) statements against the Splunk SOAR database through custom function results, allowing for reading all relevant data stored in the Splunk SOAR database and affecting system integrity. The SQL injection is possible because Splunk SOAR builds the database lookup with the supplied name instead of a bound SQL value. For more information see Manage roles and permissions in Splunk SOAR (Cloud) (https://help.splunk.com/en/splunk-soar/soar-cloud/administer-soar-cloud/manage-your-splunk-soar-cloud-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-cloud) in the Splunk documentation.	2026-08-19	6.5	CVE-2026-76364
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user who holds the "Automation Engineer" Splunk SOAR role could run arbitrary Structured Query Language (SQL) statements against the Splunk SOAR database through custom list retrieval in a playbook, allowing for create, read, update, and delete operations on all relevant data stored in the Splunk SOAR database. The SQL injection is possible because Splunk SOAR builds the custom list database lookup with the supplied list name instead of a bound SQL value. For more information see Manage roles and permissions in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-cloud/administer-soar-cloud/manage-your-splunk-soar-cloud-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-cloud) and Create custom lists for use in Splunk SOAR playbook comparisons (https://help.splunk.com/en/splunk-soar/soar-cloud/build-playbooks/manage-playbooks-and-playbook-settings/create-custom-lists-for-use-in-splunk-soar-cloud-playbook-comparisons) in the Splunk documentation.	2026-08-19	6.5	CVE-2026-76365
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user with a valid Splunk SOAR account could use Representational State Transfer (REST) API filtering on playbook runs to recover session tokens that compromise all data available to the affected user. The information disclosure is possible because Splunk SOAR does not block REST API filters from matching values that responses otherwise hide. For more information see REST Run Playbook (https://help.splunk.com/en/splunk-soar/soar-cloud/rest-api-reference/run-playbook-endpoints/rest-run-playbook) in the Splunk documentation.	2026-08-19	6.5	CVE-2026-76366
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, an authenticated user with no role assigned could use the /rest/health endpoint to gather system and cluster telemetry that should be restricted to administrative or support users. The vulnerability is a missing authorization check, where the endpoint does not verify that the caller holds a role permitted to view system health and cluster state. For more information see Manage roles and permissions in Splunk SOAR (On-premises) (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/manage-your-splunk-soar-on-premises-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-on-premises) and Monitor the health of your Splunk SOAR (On-premises) system (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/manage-your-splunk-soar-on-premises-system-health-and-	2026-08-19	4.3	CVE-2026-76360

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	performance/monitor-the-health-of-your-splunk-soar-on-premises-system) in the Splunk documentation.			
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user who holds the "Incident Commander" Splunk SOAR role could store JavaScript in a note and run it in the browser of another user when that user opens the note. The stored Cross-Site Scripting (XSS) vulnerability is possible because Splunk SOAR can treat existing note content as Hypertext Markup Language (HTML) without sanitizing that content when the note format changes. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The user who holds the "Incident Commander" Splunk SOAR role should not be able to exploit the vulnerability at will. For more information see Manage roles and permissions in Splunk SOAR (Cloud) (https://help.splunk.com/en/splunk-soar/soar-cloud/administer-soar-cloud/manage-your-splunk-soar-cloud-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-cloud) in the Splunk documentation.	2026-08-19	4	CVE-2026-76367
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, an authenticated user with restricted tenant access could use the Representational State Transfer (REST) API to view the names and identifiers of tenants that fall outside the role scope for that user. The vulnerability is possible because Splunk SOAR does not enforce role-based tenant restrictions when it returns tenant information through the REST API in deployments with multi-tenancy turned on. For more information see REST Roles and Permissions (https://help.splunk.com/en/splunk-soar/soar-cloud/rest-api-reference/role-management-endpoints/rest-roles-and-permissions) and Configure multiple tenants on your Splunk SOAR (On-premises) instance (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/7.1.0/configure-product-settings-for-your-splunk-soar-on-premises-instance/configure-multiple-tenants-on-your-splunk-soar-on-premises-instance) in the Splunk documentation.	2026-08-19	4.3	CVE-2026-76370
Splunk--Venafi app for Splunk SOAR	In versions below 2.1.4 of the Venafi app for Splunk SOAR, a user who holds a role with permission to run actions could expose keystore and private-key passwords by invoking the get certificate action, because the action's keystore_password and password parameters are not masked and are shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameters as passwords. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76385
Splunk--Zoom app for Splunk SOAR	In versions below 3.2.2 of the Zoom app for Splunk SOAR, a user who holds a role with permission to run actions could expose meeting and personal meeting ID passwords by invoking one of the create meeting, update meeting, or update user settings actions, because the affected password and pmi_password parameters are not masked and are shown in cleartext in the user interface. The information disclosure is possible because the app does not mark the affected action parameters as passwords. For more information see Run an action in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-on-premises/use-splunk-soar-on-premises/8.6.0/use-the-command-line-interface-to-perform-tasks-in-splunk-soar-on-premises/run-an-action-in-splunk-soar-on-premises).	2026-08-19	4.3	CVE-2026-76386
Spring--Spring AI	In Spring AI's tool calling support, the per-request tool list is advertised to the model as a boundary but is not fully enforced when a tool call is dispatched. Under certain conditions, a tool that was not made available to the current request could be invoked, potentially leading to privilege escalation. Affected versions: Spring AI: 2.0.0 Spring AI: 1.1.0 through 1.1.8 Spring AI: 1.0.0 through 1.0.9	2026-08-21	6.5	CVE-2026-59318

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring AI	In Spring AI's Semantic Cache support, the context hash used to isolate cached responses between different system prompts could allow cached responses to be shared across unrelated contexts. Affected versions: Spring AI: 2.0.0	2026-08-21	4.2	CVE-2026-59308
strukturag--libheif	libheif is a HEIF and AVIF file format decoder and encoder. In 1.23.0 and earlier, a crafted image sequence with a 2x2 primary plane and a 256x256 auxiliary alpha plane can cause attacker-controlled heap corruption during a normal decode and re-encode workflow. Track_Visual::decode_next_image_sample() calls transfer_channel_from_image_as() without checking that the auxiliary alpha dimensions match the main frame. The resulting inconsistent image reaches heif_track_decode_next_image() and then heif_context_encode_image(). In unc_encoder::encode(), unc_encoder_component_interleave::encode_tile() sizes its buffer with compute_tile_data_size_bytes() using the primary dimensions but copies each component using its actual plane dimensions. The oversized alpha plane is therefore copied beyond the allocation, causing an out-of-bounds write; the inverse size mismatch can also produce an out-of-bounds read. This issue is fixed in version 1.23.1.	2026-08-18	5.3	CVE-2026-62291
strukturag--libheif	libheif is a HEIF and AVIF file format decoder and encoder. In 1.23.0 and earlier, a crafted HEIF or AVIF file containing a clean aperture box can reduce an image dimension to zero and crash or corrupt tiling results when heif_image_handle_get_image_tiling(handle, 1, &tiling) is called. ImageItem::get_heif_image_tiling() returns already transformed dimensions, and process_image_transformations_on_tiling() applies the clean aperture transformation again. The second application passes zero to Box_clap::left_rounded(0), where image_width minus one underflows and constructs Fraction(0xFFFFFFFF, 2). Debug builds reach an assertion and abort, while release builds can return a corrupt crop and zero-width tiling result. The affected implementation spans libheif/image-items/image_item.cc, libheif/context.cc, and libheif/box.cc. This issue is fixed in version 1.23.1.	2026-08-18	4.3	CVE-2026-62289
strukturag--libheif	libheif is a HEIF and AVIF file format decoder and encoder. In 1.23.0 and earlier, a crafted HEIF sequence accepted by heif_context_read_from_memory() can leave the context with no registered sequence tracks and crash when heif_context_get_track(ctx, 0) is called. HeifContext::get_track() in libheif/context.cc executes assert(has_sequence()) before its normal error handling, so assert-enabled builds abort instead of allowing the public wrapper in libheif/api/libheif/heif_sequences.cc to return null. In release builds, removing the assertion lets the track_id zero path dereference m_tracks.begin()->second on an empty map, which is undefined behavior and typically crashes. The issue is reachable through documented public APIs after parsing attacker-controlled bytes. This issue is fixed in version 1.23.1.	2026-08-18	4.3	CVE-2026-62377
Stylemix--MasterStudy LMS	Subscriber Privilege Escalation in MasterStudy LMS <= 3.7.41 versions.	2026-08-18	6.3	CVE-2026-68568
Stylemix--MasterStudy LMS	Subscriber Broken Access Control in MasterStudy LMS <= 3.7.41 versions.	2026-08-18	6.5	CVE-2026-73404
sumatrapdfreader--sumatrapdf	SumatraPDF is a multi-format reader for Windows. In 3.6.1 and earlier, a crafted CHM file can supply malformed LZX Huffman code lengths to make_decode_table in ext/CHMLib/lzx.c. In the long-code branch, the function writes new internal nodes through next_symbol before validating that the canonical Huffman table has overflowed. The PRETREE case can write beyond the 104-entry PRETREE_table into adjacent heap state in struct LZXstate when reached through chm_open, chm_retrieve_object, LZXdecompress, and BUILD_TABLE. This produces heap memory corruption in the parser process, while arbitrary code execution has not been demonstrated. No fixed version is available as of this review.	2026-08-20	6.6	CVE-2026-55586
supsysitic--Contact Form by Supsysitic	Unauthenticated Bypass Vulnerability in Contact Form by Supsysitic < 1.10.0 versions.	2026-08-18	6.5	CVE-2026-73379

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ThemeGoods--Altair	Unauthenticated Broken Access Control in Altair <= 5.2.2 versions.	2026-08-20	6.5	CVE-2025-53999
Themeum--WP Crowdfunding	Subscriber Insecure Direct Object References (IDOR) in WP Crowdfunding < 2.2.1 versions.	2026-08-18	6.5	CVE-2026-73189
Themewinter--WP Cafe Pro	Author Local File Inclusion in WP Cafe Pro < 3.0.15 versions.	2026-08-20	6.6	CVE-2026-66586
themifyme--Themify Builder	The Themify Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 7.8.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to modify the stored Themify Builder styling data (padding and margin properties) of arbitrary posts, including private and draft posts, by supplying an attacker-controlled post ID and JSON styling payload. The nonce required by the handler is automatically emitted to all frontend pages rendered by the builder via wp_localize_script, meaning any unauthenticated visitor can trivially retrieve a valid nonce from page source and satisfy the only access control in place.	2026-08-22	5.3	CVE-2026-75027
thorsten--phpMyFAQ	phpMyFAQ before 4.1.6 does not adequately sanitize HTML in FAQ answers before generating PDFs via TCPDF. An attacker with permission to create or edit FAQ content can embed an tag whose src references a local file under the web root's content/ directory (e.g., content/core/config/database.php). When the PDF is generated, phpMyFAQ attempts to read the referenced file; because it is not a valid image the resulting error is converted into an uncaught exception whose stack trace discloses part of the file's contents to any user who triggers the PDF export. By default the disclosed portion is truncated (zend.exception_string_param_max_len), but a larger configured value can result in disclosure of entire files, including database credentials.	2026-08-19	6.5	CVE-2026-76210
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7 contains an authentication bypass vulnerability in SetupController that allows unauthenticated attackers to run database migrations and create configuration backups when maintenance mode is enabled. Attackers can call POST /api/setup/update-database and POST /api/setup/backup endpoints to execute database updates, disable maintenance mode, and extract database credentials from generated ZIP archives.	2026-08-19	5.3	CVE-2026-75919
thorsten--phpMyFAQ	phpMyFAQ before v4.1.6 writes content backup ZIP archives to the web-accessible document root at content.zip, exposing sensitive files including database credentials. Unauthenticated attackers can race concurrent requests to download the temporary ZIP file before deletion, or exploit XSS in admin contexts to trigger authenticated backups and retrieve the archive.	2026-08-19	5.3	CVE-2026-75920
thorsten--phpMyFAQ	phpMyFAQ versions before 4.1.7 fail to validate active status in the PDF export endpoint, allowing unauthenticated attackers to retrieve draft FAQ metadata. Attackers can access the public PDF export route with sequential FAQ identifiers to obtain titles, solution IDs, author names, and last-update timestamps of inactive or unpublished FAQs.	2026-08-19	5.3	CVE-2026-76206
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7, when configured to use PostgreSQL via the native pgsql PHP extension, declares an incorrect LIKE ESCAPE character ('=') in the Search/Database/Pgsql.php backend while escapeLikeWildcards() escapes user input with the ' ' prefix. As a result, wildcard escaping is a no-op and user-supplied % and _ characters remain active LIKE wildcards. An unauthenticated attacker can submit such characters in the public FAQ search form to force maximally broad pattern matches and expensive sequential scans, resulting in a denial of service. The PDO PostgreSQL backend is not affected, and quotes remain escaped so this does not enable quote-breaking SQL injection or data exfiltration.	2026-08-19	5.3	CVE-2026-76212

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7 fails to apply parent FAQ visibility checks before returning child resources including comments and attachments. Unauthenticated attackers can retrieve restricted comment text, commenter email addresses, and attachment filenames for FAQ records they cannot directly access by querying the comments and attachments API endpoints.	2026-08-19	5.3	CVE-2026-76215
thorsten--phpMyFAQ	phpMyFAQ versions before v4.1.6 fail to validate the security.enableRegistration setting in API endpoints, allowing attackers to create user accounts when registration is disabled. Attackers can bypass the registration restriction by submitting requests to POST /api/register or POST /api/v3.1/register endpoints, which do not check the configuration flag enforced by the HTML registration page.	2026-08-19	4.3	CVE-2026-76209
thorsten--phpMyFAQ	phpMyFAQ before 4.1.7 fails to properly enforce CONFIGURATION_EDIT permission on admin API read endpoints for LDAP, Elasticsearch, OpenSearch, and dashboard configuration, allowing any authenticated user to access sensitive administrative data. Attackers can retrieve LDAP server topology, bind account names, search bases, index statistics, and site analytics by calling these endpoints with a valid session.	2026-08-19	4.3	CVE-2026-76211
tinacms--tinacms	Tina is a headless content management system. Prior to 2.5.2, the TinaCMS CLI package's Vite dev server packages/@tinacms/cli/src/next/vite/cors.ts origin callback returns false for a disallowed origin but does not reject the request, and packages/@tinacms/cli/src/next/vite/plugins.ts still routes POST /media/upload/* to mediaRouter.handlePost. The upload code in packages/@tinacms/cli/src/next/commands/dev-command/server/media.ts writes attacker-controlled multipart contents inside the configured media root. A remote attacker can cause a developer's browser to submit this state-changing request by inducing the developer to visit an attacker-controlled page while tinacms dev is running. This issue is fixed in version 2.5.2.	2026-08-19	6.5	CVE-2026-63123
tinacms--tinacms	Tina is a headless content management system. Prior to next-tinacms-s3 23.0.4, next-tinacms-dos 23.0.4, next-tinacms-azure 14.0.4, and next-tinacms-cloudinary 26.0.4, the first-party production media adapters pass attacker-controlled object keys to storage SDK upload and delete operations without enforcing the operator's configured mediaRoot. In packages/next-tinacms-s3/src/handlers.ts, createMediaHandler accepts req.query.key for a signed PutObject URL and the DELETE path uses req.query.media as the DeleteObjectCommand key. The same missing key-boundary check exists in packages/next-tinacms-dos/src/handlers.ts, packages/next-tinacms-azure/src/handlers.ts, and packages/next-tinacms-cloudinary/src/handlers.ts. An authenticated CMS editor can therefore create or delete objects anywhere the deployment's storage credential can reach, including other tenants' or non-media objects. These issues are fixed in next-tinacms-s3 23.0.4, next-tinacms-dos 23.0.4, next-tinacms-azure 14.0.4, and next-tinacms-cloudinary 26.0.4.	2026-08-19	5.4	CVE-2026-59992
torproject--Tor	tor before 0.4.9.9 was prone to a NULL write after free when sending a CONFLUX_SWITCH cell fails. The return value of relay_send_command_from_edge() was ignored, so a send failure (which calls circuit_mark_for_close() and removes the leg via cfx_del_leg()) would go undetected, causing the caller to write to the now-freed current leg and resulting in a crash. This is TROVE-2026-017.	2026-08-20	6.5	CVE-2026-77641
torproject--Tor	Tor before 0.4.9.11 is prone to a use-after-free (and potential double free) of a conflux object when a recovery leg revives a conflux set whose last linked leg has already been closed. A malicious exit node could use this to crash a client. This is TROVE-2026-026.	2026-08-20	5.9	CVE-2026-77587
torproject--Tor	Tor before 0.4.9.9 was prone to a compression bomb bypass where an attacker could concatenate many gzip or zlib sub-streams, each just under the per-stream detection threshold, to avoid the compression bomb check entirely. This is TROVE-2026-022.	2026-08-20	5.3	CVE-2026-77639

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
TOTOLINK--EX1200L	A security vulnerability has been detected in TOTOLINK EX1200L 9.3.5u.6146_B20201023. Affected by this issue is the function setPasswordCfg of the file /cgi-bin/cstecgi.cgi of the component Password Configuration Handler. The manipulation leads to null pointer dereference. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2026-08-17	6.5	CVE-2026-75012
TOTOLINK--EX1200L	A vulnerability was detected in TOTOLINK EX1200L 9.3.5u.6146_B20201023. This affects the function setWizardCfg of the file /cgi-bin/cstecgi.cgi. The manipulation results in null pointer dereference. The attack can be launched remotely. The exploit is now public and may be used.	2026-08-17	6.5	CVE-2026-75013
treefrogframework--treefrog-framework	A security flaw has been discovered in treefrogframework treefrog-framework up to 2.11.2. This vulnerability affects the function std::strncmp of the file src/tsessioncookiestore.cpp of the component Session Cookie Handler. The manipulation results in improper authentication. The attack can be launched remotely. A high complexity level is associated with this attack. It is stated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure.	2026-08-17	5.6	CVE-2026-19974
TRENDnet--TEW-823DRU	A weakness has been identified in TRENDnet TEW-823DRU 1.1.02b01. This vulnerability affects the function nvram_get of the component CLI Configuration Tool. This manipulation causes command injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-22	6.6	CVE-2026-77988
truelockmc--streambert	Streambert is a cross-platform Electron Desktop App to stream and download video content. From version 2.5.0 until version 2.6.0, the wyzie-open-redeem IPC handler in index.js creates the partition:wyzie-redeem Electron session and registers an onHeadersReceived hook that removes the Content-Security-Policy header from every response in that session. The redeem window also lacks a setWindowOpenHandler restriction, so script injection in sub.wyzie.io, a loaded third-party resource, or a site reached through navigation executes without CSP constraints and can affect additional windows and persistent session storage. A user must open the Wyzie API key redemption window, and exploitation requires attacker-controlled script content in a loaded page. The resulting renderer script can invoke renderer-exposed application functionality and can be chained with other vulnerabilities to access internal services or sensitive data. This issue is fixed in version 2.6.0.	2026-08-18	6.9	CVE-2026-52873
typemill--typemill	Typemill is a flat-file, Markdown-based content management system designed for informational documentation websites. Versions prior to 2.23.0 are vulnerable to stored HTML attribute injection in the page metadata fields ('og:title' and 'og:description'). An authenticated user with permission to modify page metadata can inject arbitrary HTML attributes into generated '<meta>' tags due to missing output encoding. Under certain browser or DOM interaction scenarios, this may lead to stored cross-site scripting (XSS). Version 2.23.0 fixes the issue.	2026-08-21	4.6	CVE-2026-53468
Tyrrrz--DiscordChatExporter	DiscordChatExporter saves Discord chat logs to a file. Prior to 2.47.2, the VisitEmojiAsync method in DiscordChatExporter.Core/Exporting/HtmlMarkdownVisitor.cs interpolates emoji.Name into the alt attribute and emoji.Code into the title attribute without HTML entity encoding. This affects HTML exports regardless of the markdown setting. Discord's current custom emoji name validation normally excludes attribute-breaking characters, but tampered offline input, a relaxed upstream validation rule, or another future metadata source can inject an HTML attribute and execute script when a user opens the export. This issue is fixed in version 2.47.2.	2026-08-21	4.1	CVE-2026-54681
Unleash--unleash	Unleash is an open-source feature management platform. Prior to 7.5.2, 7.6.5, and 8.0.2, the addon and integration subsystem passes the operator-controlled parameters.url value from src/lib/addons/webhook.ts and the Slack, Microsoft	2026-08-21	5.5	CVE-2026-63004

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Teams, Datadog, and New Relic integrations to Addon.fetchRetry in src/lib/addons/addon.ts without restricting loopback, link-local, private, or cloud metadata addresses. An authenticated actor with the root CREATE_ADDON or UPDATE_ADDON permission can cause the server to send requests from inside its network boundary, use integration event status as a blind probing oracle, forward Authorization, customHeaders, or DD-API-KEY values to an attacker-observed host, and deliver the feature-event JSON body to internal services. This issue is fixed in versions 7.5.2, 7.6.5, and 8.0.2.			
Unleash--unleash	Unleash is an open-source feature management platform. Prior to 8.0.3, FeatureEventFormatterMd.format in src/lib/addons/feature-event-formatter-md.ts assigns Mustache.escape to an identity function before rendering action and path templates. Because Mustache.escape is process-wide, the assignment disables escaping for subsequent Mustache.render calls in email-service.ts, webhook.ts, datadog.ts, and new-relic.ts. An editor-level user can place Slack or Microsoft Teams link syntax in an unrestricted username, trigger a feature event, and inject an attacker-labeled link into a trusted outbound notification channel, while other Mustache sinks remain unescaped until restart. This issue is fixed in version 8.0.3.	2026-08-21	4.1	CVE-2026-63466
vas3k--TaxHacker	A vulnerability was determined in vas3k TaxHacker up to 0.8.2. Impacted is the function buildImapConfig of the file lib/email-sync/imap-client.ts of the component Email Sync. Executing a manipulation of the argument host/port can lead to server-side request forgery. It is possible to launch the attack remotely. The pull request to fix this issue awaits acceptance.	2026-08-23	6.3	CVE-2026-78061
veracrypt--VeraCrypt	VeraCrypt provides disk encryption with strong security based on TrueCrypt. Prior to 1.26.29, non-default builds created with WOLFCRYPT=1 and WOLFCRYPT_BACKEND route SHA-256 and SHA-512 volume-header key derivation through derive_key_sha256 and derive_key_sha512 in src/Crypto/wolfCrypt.c, where the configured iterations value is discarded and wc_HKDF is used instead of PBKDF2-HMAC. Changing the PIM or iteration count therefore does not increase derivation cost, allowing an attacker with an affected container, disk image, or volume header to perform substantially cheaper offline password guesses. Official precompiled VeraCrypt binaries and normal distribution packages use the standard PBKDF2 backend and are not affected. Volumes created by an affected WOLFCRYPT=1 build require backup and recreation because corrected builds derive different keys. This issue is fixed in version 1.26.29.	2026-08-21	6.2	CVE-2026-53762
VictoriaMetrics--VictoriaMetrics	VictoriaMetrics is a scalable solution for monitoring and managing time series data. Prior to 1.122.25, 1.136.12, and 1.146.0, vmrestore does not validate backup part path components before using lib/backup/actions/restore.go and lib/backup/fslocal/fslocal.go to write restored data below storageDataPath. An attacker who can supply or modify an S3, GCS, Azure Blob Storage, or other backup source can place .. components in object names. When an operator restores that source, the crafted names can create or overwrite files outside the intended restore root within the filesystem permissions of the vmrestore process. This issue is fixed in versions 1.122.25, 1.136.12, and 1.146.0.	2026-08-20	6.8	CVE-2026-61625
vitessio--vitess	Vitess is a database clustering system for horizontal scaling of MySQL. In 24.0.2 and earlier, the /debug/vrlog endpoint registered by addHttpEndpoint() in go/vt/vttablet/tabletmanager/vreplication/vrlog.go invokes vrlogStatsHandler() without acl.CheckAccessHTTP(r, acl.DEBUGGING), unlike comparable debug endpoints. A remote caller who can reach the vttablet debug HTTP port can bypass the configured security policy and stream VrLogStats data produced from NewVrLogStats().Send(), including literal SQL statements and bound application values from MoveTables, Reshard, Materialize, and vitess-strategy Online DDL workflows	2026-08-18	5.3	CVE-2026-65959
vllm-project--vllm	vLLM is an inference and serving engine for large language models. Prior to 0.26.0, the MiMoV2OmniMultiModalProcessor in	2026-08-17	6.5	CVE-2026-73560

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vllm/transformers_utils/processors/mimo_v2_omni.py passes attacker-controlled image and audio strings through _fetch_image, requests.get, and Image.open instead of MediaConnector, bypassing allowed_media_domains and allowed_local_media_path protections and allowing server-side requests and reads of arbitrary files accessible to the vLLM process. This issue is fixed in version 0.26.0.			
vllm-project--vllm	vLLM is an inference and serving engine for large language models. Prior to 0.26.0, the /v1/completions/derender and /v1/chat/completions/derender endpoints accept caller-supplied GenerateResponse objects whose generate_responses, choices, token_ids, prompt_logprobs, logprobs.content, top_logprobs, and routed_experts structures are processed by OnlineDerenderer and tokenizer.decode before max_model_len, max_tokens, max_num_seqs, or response-size limits are enforced, allowing an authenticated API client to consume excessive CPU and memory and produce oversized responses. This issue is fixed in version 0.26.0.	2026-08-17	4.3	CVE-2026-71486
VMware--Spring	An application using Micrometer Tracing with W3C baggage propagation in the Brave bridge is vulnerable to denial of service (DoS) due to unbounded object allocation when extracting incoming baggage headers. Specifically, an application is vulnerable when all the following are true: * The application uses a vulnerable version of io.micrometer:micrometer-tracing-bridge-brave. * W3C propagation is active (either configured manually or active by default, such as in Spring Boot 3.x+). * Baggage propagation is enabled (which is the default in Spring Boot 3.x+) and a baggage manager (such as BraveBaggageManager) is configured to handle baggage fields. * The application processes requests or messages from untrusted sources with baggage headers which it normally should not, see: https://www.w3.org/TR/trace-context/#security-considerations . * Network components including the (HTTP) server that receives the request do not limit the header size or the limit is high enough to cause issues. The last two points are very important: normally this should not affect applications because they should not receive untrusted and unlimited input for baggage. * The application processes requests or messages from untrusted sources with baggage headers. When extracting baggage from the W3C baggage header, incoming entries are parsed without enforcing limits on the number of entries or header size as mandated by the W3C Baggage specification. An attacker can send requests or messages with artificially inflated baggage headers containing many key-value pairs, causing unconditional BaggageField allocations per entry. This leads to garbage collection pressure, high CPU usage, and potential application crash via OutOfMemoryError.	2026-08-21	5.3	CVE-2026-59323
VMware--Spring Micrometer	Using untrusted, non-normalized input as-is for metrics data (such as metric names, tag keys, or tag values) is a dangerous antipattern that general-purpose instrumentation should never perform. When such unsafe instrumentation is used, the application becomes vulnerable to injection and spoofing attacks because micrometer-registry-statsd and micrometer-core do not sanitize newline characters (\n, \r) by default prior to this fix. * For the StatsD registry in micrometer-registry-statsd (when using the Datadog or Etsy flavor), because the StatsD protocol is newline-delimited, this allows for line-protocol injection (cross-metric spoofing). * For LoggingMeterRegistry in micrometer-core, because metric output is printed line-by-line to log files, this allows for both metric spoofing (if downstream log-metrics scrapers or parsers ingest the log lines as separate metrics) and general log spoofing. Specifically, an application is vulnerable when all the following are true: * The application uses a vulnerable version of io.micrometer:micrometer-registry-statsd or io.micrometer:micrometer-core. * The application uses the Datadog or Etsy flavor of the StatsD registry, or uses LoggingMeterRegistry. * The application instruments meters using user-controlled, unvalidated input for metric names, tag keys, or tag values. When vulnerable, an attacker can break out of the current metric or log line by injecting line terminators. This allows them to spoof arbitrary metrics (e.g., system load, standard JVM metrics, or other business metrics) across the metrics registry	2026-08-21	5.9	CVE-2026-59296

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	namespace (either directly via StatsD protocol or via downstream log-metric scrapers/parsers), as well as inject arbitrary log entries to spoof general log records.			
volcengine--OpenViking	OpenViking debug vector scroll and count endpoints apply only account-level scoping without user-level access controls, allowing authenticated users to read all co-tenant records. Attackers can query these endpoints to retrieve private memories, resources, skills, and secret material belonging to other users in the same account without administrative privileges.	2026-08-17	6.5	CVE-2026-75480
voxel51--fiftyone	FiftyOne is an open-source platform for refining high-quality datasets and visual AI models. Prior to 1.17.0, the FiftyOne App/API server in fiftyone/server/app.py and the /media route in fiftyone/server/routes/media.py unconditionally return Access-Control-Allow-Origin: *. Because the embedded server is local and unauthenticated, a malicious website visited by the user can read cross-origin responses. The /media endpoint accepts a filesystem path, allowing a drive-by page to read files accessible to the server process and exfiltrate them without additional clicks. The allowed_origins configuration and FIFTYONE_ALLOWED_ORIGINS environment variable now make cross-origin access explicit, while the default policy is same-origin. This issue is fixed in version 1.17.0.	2026-08-21	6.3	CVE-2026-53656
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 1.0.0 until 4.14.6 and 5.0.0-beta2, HandleSecureMessage() in src/remoted/secure.c passes a pointer inside its stack buffer to ReadSecMSG(), and src/os_crypto/shared/msgs.c decompresses up to OS_MAXSTR bytes at that offset. For an encrypted agent message on TCP port 1514 that expands to 65,536 bytes, os_zlib_uncompress() writes a terminating null byte beyond the end of the destination buffer. The resulting stack out-of-bounds write in the root-level remoted daemon can crash message processing and disrupt agent communications. This issue is fixed in versions 4.14.6 and 5.0.0-beta2.	2026-08-19	5.3	CVE-2026-44254
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.0.0 until 4.14.6 and 5.0.0-beta2, AuthenticationManager.check_user() in framework/wazuh/rbac/orm.py performs check_password_hash() only when the supplied username exists. A nonexistent username returns immediately, while a valid username causes an expensive bcrypt calculation. An unauthenticated remote attacker can compare authentication response times to enumerate valid Wazuh usernames and use that information in subsequent credential attacks. This issue is fixed in versions 4.14.6 and 5.0.0-beta2.	2026-08-19	5.3	CVE-2026-44255
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.4.0 until 4.14.6 and 5.0.0-beta2, api/api/middlewares.py decodes the Basic authentication username before credential validation and passes it to the access logger without neutralizing control characters. api/api/alogging.py interpolates that value into the plain-text API log. An unauthenticated attacker can include carriage returns or line feeds in the username to forge entries, obscure activity, or poison systems that consume the plain-text audit log. The JSON log format is not affected because JSON serialization escapes these characters. This issue is fixed in versions 4.14.6 and 5.0.0-beta2.	2026-08-19	5.3	CVE-2026-44256
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 4.6.0 until 4.14.6 and 5.0.0-beta3, DB::getFile() and DB::searchFile() in src/syscheckd/src/db/src/file.cpp concatenate a monitored file path into SQLite row filters. On non-Windows systems, FIMDBCreator::encodeString() does not escape the value. A local user who can create a filename in a File Integrity Monitoring directory can inject a UNION SELECT expression when wazuh-syscheckd processes or deletes that path. The confirmed primitive manipulates SELECT result sets consumed by the FIM code; stacked statements and remote code execution were not demonstrated. This issue is fixed in versions 4.14.6 and 5.0.0-beta3.	2026-08-19	5.3	CVE-2026-49392

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wazuh--wazuh	Wazuh is a free and open source platform used for threat prevention, detection, and response. From 3.9.0 until 4.14.5 and 5.0.0-beta2, the Wazuh cluster protocol in framework/wazuh/core/cluster/common.py allows an authenticated cluster node to exhaust memory on the master. The receive_str() method accepts an attacker-controlled total for InBuffer without a maximum, so a new_str command can request a multi-gigabyte bytearray and repeated requests accumulate in in_str. The divided-message path also retains flag_divided fragments under unique counters in div_msg_box without a count, aggregate-size, or expiration limit. Exploitation can disrupt agent connectivity and alert processing across the monitored environment. This issue is fixed in versions 4.14.5 and 5.0.0-beta2.	2026-08-19	4.9	CVE-2026-44253
Wazuh--wazuh-manager	Wazuh 4.0.0 before 4.14.7 and 5.0.0-beta2 contain a denial of service vulnerability that allows authenticated attackers with allow_run_as enabled to exhaust CPU resources by submitting arbitrarily deeply nested JSON structures to the POST /security/user/authenticate/run_as endpoint. Attackers can repeatedly submit malformed auth_context bodies with unlimited nesting depth to cause the API framework to consume excessive CPU, denying service to all other API consumers.	2026-08-18	6.5	CVE-2026-74039
Wazuh--wazuh-manager	Wazuh 4.0.0 before 4.14.6 contains a path traversal vulnerability that allows authenticated cluster peers to delete arbitrary directory contents by supplying a traversal-shaped node name in the cluster hello payload without validation. Attackers holding a valid cluster Fernet key can craft a malicious node name and disconnect, triggering the master's peer cleanup routine to remove the contents of arbitrary directories within the Wazuh installation path writable by the wazuh user.	2026-08-18	6.5	CVE-2026-74044
Wazuh--wazuh-manager	Wazuh 4.4.0 before 4.14.7 contains a denial of service vulnerability in the fdecompress_files() function within cluster.py that allows authenticated cluster peers to exhaust memory by supplying a malicious synchronization archive without decompressed size limits. Attackers holding a valid cluster Fernet key can upload a small, highly compressed zip bomb archive that forces wazuh-clusterd on the master node to decompress the full payload into memory, causing memory exhaustion and service disruption.	2026-08-18	4.9	CVE-2026-74046
WebAppick--CTX Feed	Shop manager Arbitrary File Download in CTX Feed <= 6.6.47 versions.	2026-08-18	4.9	CVE-2026-73383
Webkul--Bagisto	A vulnerability was found in Webkul Bagisto up to 2.4.4. Affected by this issue is some unknown functionality of the file /admin/configuration/cache-management/execute of the component Configuration Management. The manipulation of the argument action results in authorization bypass. The attack may be launched remotely. The exploit has been made public and could be used. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."	2026-08-17	6.3	CVE-2026-19994
Webkul--Bagisto	A vulnerability has been found in Webkul Bagisto up to 2.4.4. Affected by this vulnerability is an unknown functionality of the file /customer/account/rma/update-status of the component RMA State Validation. The manipulation leads to enforcement of behavioral workflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."	2026-08-17	4.3	CVE-2026-19993
Webkul--Bagisto	A vulnerability was identified in Webkul Bagisto up to 2.4.4. This vulnerability affects unknown code of the file /admin/customers of the component Backend Customer Behavior Data Endpoint. Such manipulation of the argument ID leads to	2026-08-17	4.3	CVE-2026-19996

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	improper privilege management. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."			
Webkul--Bagisto	A security flaw has been discovered in Webkul Bagisto up to 2.4.4. This issue affects some unknown processing of the file /admin/sales/rma/requests of the component Backend Sales RMA Endpoint. Performing a manipulation results in authorization bypass. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."	2026-08-17	4.7	CVE-2026-19997
Webkul--Bagisto	A vulnerability was detected in Webkul Bagisto up to 2.4.4. Impacted is an unknown function of the file /customer/account/rma/store. The manipulation of the argument rma_qty/resolution_type/rma_reason_id results in enforcement of behavioral workflow. The attack may be performed from remote. The exploit is now public and may be used. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."	2026-08-17	4.3	CVE-2026-75081
Webkul--Bagisto	A flaw has been found in Webkul Bagisto up to 2.4.4. The affected element is an unknown function of the file /customer/register of the component Customer-Registration Notification Email. This manipulation of the argument first_name/last_name causes basic cross site scripting. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."	2026-08-18	4.3	CVE-2026-75082
webtoffee-- WebToffee WooCommerce PDF Invoices, Packing Slips, Delivery Notes & Shipping Labels	The WebToffee WooCommerce PDF Invoices, Packing Slips, Delivery Notes & Shipping Labels plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 4.9.8 via the get_image_src_in_base64 function. This makes it possible for authenticated attackers, with subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. The base64-encoded file contents are embedded into the cached invoice HTML and served directly to the attacker via the plugin's own Print/Download invoice endpoints, which require only a valid nonce and access key.	2026-08-22	6.5	CVE-2026-18027
weechat--weechat	WeeChat (Wee Enhanced Environment for Chat) is a free chat client. In versions 4.3.0 through 4.9.0, the WeeChat relay module's WebSocket permmessage-deflate decompression function relay_websocket_inflate() has no upper bound on output size. An authenticated relay user can send a small compressed WebSocket frame (~100 bytes) that decompresses to gigabytes, exhausting all server memory and crashing the entire WeeChat process. The api protocol enables permmessage-deflate and requires authentication before WebSocket upgrade. Version 4.9.1 patches the issue.	2026-08-21	6.5	CVE-2026-53524
wekan--wekan	Wekan is open source kanban built with Meteor. From 9.57 until 9.74, the /api/boards/:boardId/exportExcel route in models/exportExcel.js called the	2026-08-19	6.5	CVE-2026-68559

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	asynchronous exporterExcel.canExport(user) authorization guard from models/server/ExporterExcel.js without awaiting it. The returned Promise was always truthy, so exporterExcel.build(res) ran even when board.isVisibleBy(user) would deny access, allowing any authenticated non-member to download private board card titles, descriptions, lists, swimlanes, members, and metadata. This issue is fixed in version 9.74.			
wekan--wekan	Wekan is open source kanban built with Meteor. Prior to 10.38, the /api/boards/:boardId/export, /api/boards/:boardId/attachments/:attachmentId/export, /api/boards/:boardId/export/csv, and /api/boards/:boardId/exportExcel handlers in models/export.js and models/exportExcel.js looked up a user from the attacker-controlled authToken query parameter and immediately called user._id.toString() without checking whether ReactiveCache.getUser() returned undefined. A request for a private board with an unknown token therefore threw a TypeError from an asynchronous route, producing an unhandled rejection that could terminate the Wekan process and deny service to all users. Version 10.38 adds a 401 guard after every export token lookup and wraps export handlers with safeRoute() so unexpected exceptions become controlled responses. This issue is fixed in version 10.38.	2026-08-19	6.5	CVE-2026-68901
Wireshark Foundation--Wireshark	Bluetooth AVRCP Profile protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	5.5	CVE-2026-76917
Wireshark Foundation--Wireshark	SSH protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	5.5	CVE-2026-76918
Wireshark Foundation--Wireshark	ESS protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	5.3	CVE-2026-76919
Wireshark Foundation--Wireshark	CMS protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	5.5	CVE-2026-76921
Wireshark Foundation--Wireshark	Bluetooth BR/EDR FHS protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	5.5	CVE-2026-76922
Wireshark Foundation--Wireshark	Bluetooth HFP Profile protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	5.5	CVE-2026-76923
Wireshark Foundation--Wireshark	Kerberos protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	5.5	CVE-2026-76924
Wireshark Foundation--Wireshark	CMS protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	4.7	CVE-2026-76881
Wireshark Foundation--Wireshark	Bluetooth Attribute Protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	4.7	CVE-2026-76882
Wireshark Foundation--Wireshark	Catapult DCT2000 file parser crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	4.7	CVE-2026-76883

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Wireshark Foundation--Wireshark	UMTS FP protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	4.7	CVE-2026-76889
Wireshark Foundation--Wireshark	3gpp phone log file parser crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	4.7	CVE-2026-76920
Wireshark Foundation--Wireshark	H.245 protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	4.7	CVE-2026-76927
Wireshark Foundation--Wireshark	Pcapng file parser crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	4.7	CVE-2026-76929
withastro--astro	Astro is a web framework for content-driven websites. From 10.0.3 until 11.0.3, the Astro Vercel adapter in packages/integrations/vercel/src/serverless/entrypoint.ts accepts x_astro_path for the public /_isr function based only on the x-vercel-isr header, allowing unauthenticated GET requests to render routes protected only by Vercel edge path rules or split edge middleware. This issue is fixed in 11.0.3.	2026-08-17	6.5	CVE-2026-73424
WP Legal Pages--WP Cookie Notice for GDPR, CCPA & ePrivacy Consent	Subscriber Cross Site Scripting (XSS) in WP Cookie Notice for GDPR, CCPA & ePrivacy Consent <= 4.3.9 versions.	2026-08-18	6.5	CVE-2026-73359
WP Table Builder--WP Table Builder	Contributor Broken Access Control in WP Table Builder <= 2.2.0 versions.	2026-08-18	4.3	CVE-2026-74006
wpchill--Image Photo Gallery Final Tiles Grid	The Image Photo Gallery Final Tiles Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'delay' shortcode attribute in all versions up to, and including, 3.6.12 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-22	6.4	CVE-2026-4559
wpdevart--Booking calendar, Appointment Booking System	Unauthenticated Insecure Direct Object References (IDOR) in Booking calendar, Appointment Booking System <= 3.2.36 versions.	2026-08-18	6.5	CVE-2026-73395
WPDeveloper--Table Of Contents Block	Contributor Cross Site Scripting (XSS) in Table Of Contents Block <= 1.5.0 versions.	2026-08-18	6.5	CVE-2026-66645
wpeverest--User Registration	Subscriber Broken Authentication in User Registration <= 5.2.6 versions.	2026-08-18	5.4	CVE-2026-73995
wpmonks--Gravity Booster- Styles & Layouts for Gravity Forms	Subscriber Broken Access Control in Gravity Booster – Styles & Layouts for Gravity Forms <= 6.0 versions.	2026-08-18	5.4	CVE-2026-74004
wpsoul--Greenshift animation and page builder blocks	The GreenShift - Animation and Page Builder Blocks plugin for WordPress is vulnerable to unauthorized modification of data in versions up to, and including, 12.8.9. This is due to a missing capability check on the 'gspb_update_global_wp_settings' function that only verifies the 'edit_posts' capability instead of requiring administrative privileges. This makes it possible for authenticated attackers, with contributor-level access and above, to modify global WordPress theme color settings site-wide, leading to site defacement.	2026-08-22	4.3	CVE-2026-5093

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WPZOOM-- WPZOOM Forms Contact Form Plugin for Gutenberg	Contributor Cross Site Scripting (XSS) in WPZOOM Forms - Contact Form Plugin for Gutenberg <= 2.0.4 versions.	2026-08-18	6.5	CVE-2026-66639
wronganswersonly --Wufoo Shortcode	Contributor Cross Site Scripting (XSS) in Wufoo Shortcode <= 1.55 versions.	2026-08-18	6.5	CVE-2026-66643
WWBN--AVideo	WWBN AVideo through commit 9c39d8c8b4c1f75540788d6b391740852ceb0732 contains an authorization bypass vulnerability in the Users_affiliations add.json.php endpoint that allows authenticated users to forge two-party consent records by supplying the counterparty's agreement timestamp. Attackers can create a forged affiliation with status='a' and then reassign video ownership to arbitrary users through the videoAddNew.json.php endpoint, which trusts the forged affiliation as an authorization term.	2026-08-22	6.5	CVE-2026-58002
WWBN--AVideo	AVideo through commit 9c39d8c8 contains an information exposure vulnerability in feed/index.php that allows unauthenticated attackers to retrieve channel owner email addresses by supplying a public channel name parameter. Attackers can enumerate all creator email addresses by iterating through public channel names and extract them from the itunes:email and itunes:author RSS elements, enabling account takeover attempts and phishing campaigns.	2026-08-22	5.3	CVE-2026-56380
WWBN--AVideo	AVideo through commit 9c39d8c8 contains a cross-site request forgery vulnerability in channelToGallery.json.php that allows attackers to modify site-wide Gallery configuration by performing unauthorized writes to plugin data. Attackers can craft a cross-site GET request carrying an administrator's session cookie to promote arbitrary channels to the front page or delete curated sections without token validation.	2026-08-22	5.4	CVE-2026-57944
WWBN--AVideo	WWBN AVideo through commit 9c39d8c8 contains a cross-site request forgery vulnerability in objects/videoEditLight.php that lacks request authenticity checks and accepts GET requests. Attackers can store an img tag in a video description that transfers video ownership to an attacker-controlled account when an administrator views the video page.	2026-08-22	5.7	CVE-2026-58001
Xapian--xapian- core	A cross-site scripting vulnerability in queryparser/termgenerator_internal.cc in Xapian xapian-core before 2.1.0 and before 1.4.32 exists due to incomplete HTML escaping by Xapian::MSet::snippet(). NOTE: this issue exists because of a missed corner case of CVE-2018-0499.	2026-08-20	4.4	CVE-2026-77643
xianrendzw-- EasyReport	A security vulnerability has been detected in xianrendzw EasyReport up to 2.0.17.0522_Beta. Affected by this issue is some unknown functionality of the file ModuleController.java of the component Move Operations. Such manipulation of the argument sourcePath leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-18	6.3	CVE-2026-75876
xianrendzw-- EasyReport	A security vulnerability has been detected in xianrendzw EasyReport up to 2.0.17.0522_Beta. The affected element is the function DataSourceController.add of the file DataSourceController.java of the component QueryerFactory. Such manipulation of the argument queryerClass leads to permission issues. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-19	6.3	CVE-2026-75978
xianrendzw-- EasyReport	A vulnerability was found in xianrendzw EasyReport up to 2.0.17.0522_Beta. Affected is the function execSqlText/previewSqlText of the file DesignerController.java of the component SQL Preview Endpoint. The manipulation of the argument sqlText results in improper neutralization of special elements used in a template engine. The attack can be executed remotely. The	2026-08-19	6.3	CVE-2026-75979

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.			
Yamaha Corporation--VOCALOID6	Use of hard-coded credentials issue exists in VOCALOID6 , which may allow an attacker to impersonate a legitimate VOCALOID6 Editor and gain access to Yamaha's activation and content servers.	2026-08-21	5.3	CVE-2026-76131
yangzongzhuan--RuoYi-Vue	A vulnerability was found in yangzongzhuan RuoYi-Vue up to 3.9.2. This impacts the function fileDownload/resourceDownload of the file ruoyi-admin/src/main/java/com/ruoyi/web/controller/common/CommonController.java of the component Common Download Endpoint. Performing a manipulation of the argument fileName/resource results in path traversal. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-19	4.3	CVE-2026-76576
yawkat--lz4-java	yawkat LZ4 Java provides LZ4 compression for Java. Prior to 1.11.1, JNI-backed XXHash implementations fail to validate the byte array object and the off and len arguments in XXHashFactory.nativeInstance().hash32().hash(), XXHashFactory.nativeInstance().hash64().hash(), XXHashFactory.nativeInstance().newStreamingHash32().update(), and XXHashFactory.nativeInstance().newStreamingHash64().update(), allowing null arrays or oversized ranges to reach native code, read outside the Java array, and fatally terminate the JVM. This issue is fixed in version 1.11.1.	2026-08-18	6.5	CVE-2026-59949
ZcashFoundation--zebra	ZEBRA is a Zcash node written entirely in Rust. Prior to 4.5.0, an attacker authenticated to an enabled Zebra RPC endpoint can terminate zebrad by supplying a getblocktemplate LongPollId containing multi-byte UTF-8 characters. In zebra-rpc/src/methods/types/long_poll.rs, LongPollId::from_str originally checked the input byte length and then sliced fixed byte ranges to parse encoded fields. A slice boundary can land inside a multi-byte character and trigger Rust's byte index is not a char boundary panic. Zebra release builds use panic equals abort, so one malformed authenticated RPC request terminates the entire node process and can be repeated after restart. This issue is fixed in version 4.5.0.	2026-08-18	6.5	CVE-2026-52731
ZcashFoundation--zebra	ZEBRA is a Zcash node written entirely in Rust. Prior to 4.5.0, a natural or attacker-influenced chain fork can leave stale Sapling and Orchard note-commitment subtree roots in Zebra state. In zebra-state/src/service/non_finalized_state/chain.rs, Chain::pop_tip removed a reverted tip block but did not remove subtree entries whose end_height belonged to that block, unlike the cleanup performed by pop_root. When the winning fork later finalized, the abandoned branch's stale subtree data could be written to RocksDB and survive node restarts. The corrupted history can cause z_getsubtreesbyindex consumers such as lightwalletd and light wallets to receive incorrect subtree roots, producing wallet synchronization failures or incorrect wallet state and requiring a full state rebuild for recovery. This issue is fixed in version 4.5.0.	2026-08-18	6.5	CVE-2026-52733
ZcashFoundation--zebra	ZEBRA is a Zcash node written entirely in Rust. Prior to 4.5.0, one unauthenticated P2P peer can monopolize all 25 MAX_INBOUND_CONCURRENCY slots in Zebra's inbound mempool download and verification pipeline. In zebrad/src/components/mempool/downloads.rs, the bounded queue was shared globally without per-peer accounting, while peer identity was not carried through Gossip and FullQueue responses were mapped to Response::Nil instead of reaching overload disconnection handling. An attacker can advertise fake transaction identifiers and remain silent so each task holds a slot until TRANSACTION_DOWNLOAD_TIMEOUT, then periodically refill the queue as slots expire. While saturated, honest peer transactions and local sendrawtransaction requests are rejected with MempoolError::FullQueue, although block validation and synchronization continue. This issue is fixed in version 4.5.0.	2026-08-18	5.3	CVE-2026-52732

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ZcashFoundation--zebra	ZEBRA is a Zcash node written entirely in Rust. Prior to 4.5.0, an unauthenticated P2P peer can cause the mempool download pipeline to retain transactions after verification reaches the outer RATE_LIMIT_DELAY timeout. In zebra/src/components/mempool/downloads.rs, Downloads::poll_next removed cancel_handles entries after success and ordinary verification errors, but tokio::time::error::Elapsed did not carry the UnminedTxId needed to remove the timed-out entry. Each retained cancel_handles entry could hold a full Gossip::Tx(UnminedTx), while normal mined-transaction cleanup could not match attacker transactions and no periodic garbage collection or count cap existed. Sustained traffic therefore caused monotonic memory growth until swap pressure degraded the node or the operating system terminated the zebra process for exhausting memory. This issue is fixed in version 4.5.0.	2026-08-18	5.3	CVE-2026-52734
ZcashFoundation--zebra	ZEBRA is a Zcash node written entirely in Rust. Prior to 4.5.0, a malicious unauthenticated P2P peer can answer Zebra's outbound getblocks or FindBlocks request with a small two-hash inventory and then serve a syntactically valid block whose coinbase height is far above the local chain tip. In zebra/src/components/sync/downloads.rs, BlockDownloadVerifyError::AboveLookaheadHeightLimit originally carried only the block height and hash, so handle_block_response could not attribute the failure to the advertising peer. The error then reached the restart-worthy default path in zebra/src/components/sync.rs, cancelling all in-flight downloads from honest peers and imposing a 67-second sync restart delay on mainnet. Because the peer was neither scored nor disconnected, the peer could repeat the cycle indefinitely with minimal bandwidth and significantly degrade synchronization without corrupting state. This issue is fixed in version 4.5.0.	2026-08-18	5.3	CVE-2026-52737
ZcashFoundation--zebra	ZEBRA is a Zcash node written entirely in Rust. Prior to 4.5.0, a malicious block producer can terminate zebra by placing the same shielded transaction in a non-finalized parent block and its child. In zebra-state/src/service/non_finalized_state/chain.rs, Chain::push originally inserted the transaction hash into tx_loc_by_hash and asserted uniqueness before updating shielded data and running the duplicate Sprout, Sapling, or Orchard nullifier checks. The repeated transaction therefore reached the transactions must be unique within a single chain assertion before contextual validation could reject it cleanly. Zebra release builds use panic equals abort, so the reachable assertion terminates the entire process; exploitation requires either two consecutive attacker-mined blocks or an attacker-mined child immediately after an honest block includes the attacker's shielded transaction. This issue is fixed in version 4.5.0.	2026-08-18	5.9	CVE-2026-52739
zenitram--malla	Malla is a web analyzer for Meshtastic networks based on MQTT data. Prior to commit 4086e2b5f61615a813b70b25bc76095083552135, code names (long_name, short_name) received via MQTT are stored in SQLite without sanitization and rendered into the DOM without escaping. Any participant on a public Meshtastic MQTT broker can set a malicious node name that executes JavaScript in the browser of every Malla dashboard visitor. Commit 4086e2b5f61615a813b70b25bc76095083552135 fixes the issue.	2026-08-21	6.3	CVE-2026-43980
zephyrproject--zephyr	The Sierra Wireless HL7800 cellular modem driver (drivers/modem/vendor_standalone/hl7800.c, located at drivers/modem/hl7800.c in v4.4.0 and earlier) parses AT responses with roughly twenty handlers that call net_buf_linearize(value, sizeof(value), *buf, 0, len) into a 128-byte stack buffer and then write value[out_len] = 0. Because net_buf_linearize() (lib/net_buf/buf.c) can return a count equal to its destination-length argument, a field that exactly fills the buffer makes the terminating NUL land one byte past the end, a single-byte out-of-bounds write into adjacent stack memory. The +KCELLMEAS cell-measurement handler on_cmd_atcmdinfo_rssi() is worse: it passed the wire length len as the destination size (net_buf_linearize(value, len, *buf, 0, len)), so a response line longer than 128 bytes overflows the value stack buffer with attacker-influenceable	2026-08-18	6.4	CVE-2026-12520

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	content. The line length comes from net_buf_findcrlf(), which accumulates bytes across the whole net_buf fragment chain and is not bounded to 128, so an over-long line reaches the defect. The data originates from the cellular modem over UART, driven by the network: operator-scan results, +CGCONTRDP IP/DNS info, socket indications, and +KCELLMEAS neighbour-cell reports. An attacker able to shape what the modem emits - a rogue base station, a compromised modem baseband, or a remote peer feeding oversized response framing - can drive a line past 128 bytes. The handlers run in the driver's RX thread in kernel context, so the corruption is kernel-side. The +KCELLMEAS path is a full stack buffer overflow whose worst case is code execution in kernel context and whose floor is a reliable crash; the remaining sites are single-byte NUL out-of-bounds writes. Exploitation requires the modem to emit an over-long AT response line, giving high attack complexity over an adjacent (cellular radio) vector. The fix passes sizeof(dst) - 1 (and correct explicit bounds for the IMSI and +KCELLMEAS sites) so the terminator always stays in bounds.			
zephyrproject--zephyr	The Zephyr kernel validates the k_thread_join() and k_thread_abort() system calls (declared __syscall in include/zephyr/kernel.h) through thread_obj_validate() in kernel/thread.c. Its default switch branch is the access-denied path, taken when k_object_validate() returns -EPERM (the calling user thread was never granted access to the target thread object) or -EBADF (the supplied pointer is not a registered kernel object of the right type). That branch invoked K_OOPS(K_SYSCALL_VERIFY_MSG(ret, "access denied")), but K_SYSCALL_VERIFY_MSG treats a true expression as success; the non-zero error code ret therefore read as "verified OK", the kernel oops was never raised, and control fell through to CODE_UNREACHABLE. Because k_thread_join() and k_thread_abort() are system calls, an unprivileged user-mode thread (under CONFIG_USERSPACE) can reach this denial path directly by calling either syscall on a thread object it does not own. Instead of the offending thread being cleanly terminated, execution reaches __builtin_unreachable() while running in supervisor mode inside the syscall handler. On Clang builds CODE_UNREACHABLE emits an illegal-instruction trap, so a user thread can deterministically crash the kernel - a locally triggerable denial of service that escapes the userspace sandbox. On GCC builds the path is undefined behavior: the compiler may drop the return-value handling for thread_obj_validate(), so it can return an undefined bool; if that is false, the caller proceeds into the real k_thread_join()/k_thread_abort() implementation for a thread the user was never authorized to access, an access-control bypass. The fix changes the verification expression to ret == 0, so a denied (non-zero) result now correctly raises K_OOPS and terminates the offending caller.	2026-08-18	6.5	CVE-2026-12631
zephyrproject--zephyr	Zephyr's Precision Time Protocol receive handler ptp_msg_post_rcv() in subsys/net/lib/ptp/msg.c takes the 4-bit message type straight off the wire via ptp_msg_type() (msg->header.type_major_sdo_id & 0xF, range 0-15) and uses it to index the msg_size[] table. That table only defines entries up to PTP_MSG_MANAGEMENT (0xD), giving it ARRAY_SIZE == 14. Before the fix there was no upper-bound check, so the undefined types 0xE and 0xF indexed one or two int slots past the end of the array - an out-of-bounds read of adjacent read-only data. The out-of-bounds value is then reused as a length: it gates msg_size[type] > cnt, and when it is small or negative it makes cnt - msg_size[type] a large positive budget passed to msg_tlv_post_rcv(), whose TLV loop then walks the message suffix past the received bytes, performing further out-of-bounds reads and in-place byte-swap writes on memory beyond the message slab. The defect is reached directly from the network: ptp_port_event_gen() in subsys/net/lib/ptp/port.c reads a PTP frame with ptp_transport_rcv() and calls ptp_msg_post_rcv() with the attacker-chosen type. PTP uses UDP multicast or raw Ethernet (0x88F7) and is unauthenticated, so any host on the same link can trigger the indexing on a CONFIG_PTP-enabled node with no preconditions. The reliably reproducible impact is a denial of service (fault/crash); a limited memory-corruption path exists but depends on the build-specific value adjacent to	2026-08-18	6.5	CVE-2026-12632

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	msg_size[], which the attacker cannot tune. The fix rejects type >= ARRAY_SIZE(msg_size) with -EBADMSG before any indexing.			
zephyrproject--zephyr	The WNC-M14A2A LTE-M modem driver mishandles unsolicited %NOTIFYEV: events in on_cmd_socknotifyev() (drivers/modem/vendor_standalone/wncm14a2a.c). The response line is linearized into a fixed 40-byte stack buffer via net_buf_linearize(), which caps the copy at 39 bytes and returns out_len <= 39. The two quote-delimiter scanning loops, however, were bounded by len - the full CR/LF-delimited frame length returned by net_buf_findcrLf() - rather than by out_len. When a %NOTIFYEV: line longer than 39 bytes contains no " within the linearized region, the loop indices p1/p2 walk past value[39] and read adjacent stack memory until a stray quote byte is found or the index reaches len. The over-read string is then passed to strncmp()/atoi()/LOG_*, and if a quote byte is found out of bounds the subsequent value[p2] = '\0' performs a single-NUL out-of-bounds stack write at an attacker-influenced offset. The %NOTIFYEV: payload carries network-derived content (LTIME network time, SIB1 base-station system information, CSPA/RRSTATE), so a rogue cellular base station, a malicious or compromised modem module, or RF manipulation that induces an over-long notify line reaches the defect without any application interaction; the handler runs automatically on the unsolicited event in the modem RX thread. The impact is out-of-bounds stack disclosure (into logs and parsing) and stack corruption that can crash the modem RX thread (denial of service). The write offset is only weakly controlled, so memory-safe code execution is not demonstrated. The fix bounds both scanning loops by out_len, keeping all accesses within the linearized buffer.	2026-08-17	5	CVE-2026-12519
zephyrproject--zephyr	The NVS backend of the Zephyr settings subsystem (subsys/settings/src/settings_nvs.c) reads stored setting-name entries into fixed 74-byte stack buffers and NUL-terminates them with buf[rc] = '\0', where rc is the return value of nvs_read(). Per its contract, nvs_read() returns the full stored entry length (wlk_aten.len), which can exceed the supplied buffer length - only MIN(len, stored_len) bytes are actually copied, but the return value may be much larger, bounded only by the NVS sector size. Three sites (settings_nvs_cache_match(), settings_nvs_load(), and settings_nvs_save()) used this value directly as the NUL index without clamping, so an oversized stored name entry causes a single \0 byte to be written past the end of the stack buffer at an attacker-influenced offset (CWE-787). The oversized entry cannot arise through the normal settings API, where names are bounded by SETTINGS_MAX_NAME_LEN. It requires an actor able to write the flash that backs the settings partition - a co-resident or untrusted component sharing the flash device, a malicious settings image/restore, or offline/physical flash access (a shared-flash threat model). The malformed entry is parsed when settings_load() runs at boot or subsystem init, or during settings_save(). The out-of-bounds write is a single NUL byte at an offset equal to the crafted entry length (up to the NVS sector size), so the practical impact is a crash or denial of service and limited stack corruption rather than reliable code execution. There is no confidentiality impact, and the path is not reachable from the network through the ordinary settings interface. The fix skips any entry whose nvs_read() length is greater than or equal to the buffer size before performing the NUL store.	2026-08-19	5.3	CVE-2026-12634
zephyrproject--zephyr	The Infineon Airoc Wi-Fi driver's transmit callback airoc_mgmt_send() in drivers/wifi/infineon/airoc_wifi.c allocates a net_buf from the fixed airoc_pool for every outbound packet. When whd_network_send_ethernet_data() returns a synchronous failure, the underlying WHD library does not take ownership of the buffer, but the pre-fix driver returned -EIO without releasing it. Each failed transmit therefore permanently leaks one buffer from the pool. airoc_pool is small and fixed (AIROC_WIFI_TX_PACKET_POOL_COUNT + AIROC_WIFI_RX_PACKET_POOL_COUNT, default 20 buffers) and is shared by WHD's whd_host_buffer_get callback for both transmit and receive. Once enough send failures have leaked the pool dry, airoc_wifi_host_buffer_get() returns	2026-08-22	5.3	CVE-2026-12999

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WHD_BUFFER_ALLOC_FAIL for all subsequent allocations, so both transmit and the WHD-driven receive path fail and Wi-Fi connectivity is lost until the device is rebooted. The leak occurs only on the transmit error path. A Wi-Fi-adjacent attacker can influence the conditions that cause synchronous send failures (for example by deauthenticating/disassociating the station while the local stack continues to attempt transmits), and ordinary transient failures over the device's lifetime accumulate toward the same state. Reliable on-demand triggering is of high complexity and the impact is availability-only, but the resulting denial of service is permanent and non-recoverable without a reboot. The fix releases the buffer with airoc_wifi_buffer_release() on the failure branch, returning it to the pool. The commit also removes a redundant k_sem_give() in airoc_mgmt_disconnect(); because data->sema_common is a binary semaphore (limit 1) the duplicate give merely saturated at 1 and had no security impact.			
zephyrproject--zephyr	The ARM PL011 UART driver in drivers/serial/uart_pl011.c fails to acknowledge receive error interrupts. On the PL011, the framing, parity, break, and overrun error interrupts (PL011_IMSC_ERROR_MASK) are cleared only by writing the interrupt-clear register URTICR; reading the data register clears the RX interrupt and the per-byte RSR status but not the error interrupt status in MIS. The interrupt service routine pl011_isr() acknowledged only the CTS modem-status interrupt and never wrote icr for the error bits, so an asserted error interrupt remains pending after the ISR returns. When an application enables error-interrupt reporting via the public uart_irq_err_enable() API, an attacker who controls the serial peer can deterministically assert these error bits by injecting line errors on the RX line - a baud/stop-bit mismatch or mid-character break (framing/break error), a flipped parity bit (parity error), or FIFO flooding (overrun error). Because the error interrupt is never cleared, the interrupt line stays asserted and the CPU re-enters pl011_isr() immediately and indefinitely, producing an interrupt-storm livelock from which the core makes no forward progress. The impact is an availability-only denial of service (permanent hang), reachable from an external or removable UART peer. Exploitation is gated by configuration: the error interrupt is off by default and no in-tree subsystem enables it, so only applications that explicitly call uart_irq_err_enable() on a PL011-based, interrupt-driven port are affected. The fix makes pl011_isr() acknowledge the pending error bits via uart->icr, breaking the loop, and additionally clears the latched RSR status in pl011_err_check().	2026-08-17	4.6	CVE-2026-12629
zephyrproject--zephyr	Zephyr's 6LoWPAN IP Header Compression (IPHC) uncompression code contains an out-of-bounds read in get_ihpc_inlined_size() (subsys/net/ip/6lo.c). The destination inline size is looked up in da_inline_size_table, which has 13 entries, using an index built from the M, DAC and DAM bits of the received IPHC dispatch word (iphc & NET_6LO_IPHC_DA_MASK, a 4-bit value of 0-15). The reserved combinations 13, 14 and 15 are not bounds-checked and read past the end of the table. The iphc word is taken directly from the received frame, and get_ihpc_inlined_size() is reached on every inbound 6LoWPAN frame via net_6lo_uncompress() from the 802.15.4 receive path (subsys/net/l2/ieee802154/ieee802154_6lo.c and ieee802154_6lo_fragment.c). An unauthenticated attacker on the radio/adjacent link can therefore craft a frame whose destination addressing-mode nibble selects an out-of-range index, with no privileges or user interaction. The out-of-bounds value becomes the computed inline_size, which then drives header reconstruction before the buffer-length check: it is used to dereference *(pkt->buffer->data + sizeof(iphc) + inline_size) and to compute a size_t diff that can underflow, leading to a further out-of-bounds read of the packet buffer and malformed uncompression. The practical impact is a radio-triggerable out-of-bounds read / denial-of-service on the receiver; the leaked byte is not returned to the attacker. The fix rejects any destination index beyond the table, aborting processing of the malformed frame.	2026-08-17	4.3	CVE-2026-12630
Znuny--Znuny	Znuny before LTS 6.5.22 allows AgentTicketEmailResend template XSS.	2026-08-20	4.8	CVE-2026-77506

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. Versions prior to 3.2.10, 3.3.12 and 3.4.13 contain a heap out-of-bounds write in <code>Imf_4_0::SampleCountChannel::set(int r, unsigned int newNumSamples[])</code> . The row-based sample-count setter computes the target Y coordinate with <code>dataWindow.min.x</code> instead of <code>dataWindow.min.y</code> . For a valid deep image data window where <code>min.x != min.y</code> , a valid row index can be translated into an invalid Y coordinate, causing writes before the allocated <code>_numSamples</code> buffer. The vulnerability is reachable through the public <code>OpenEXRUtil DeepImage</code> API and can lead to heap corruption and process crashes. This issue has been fixed in versions 3.2.10, 3.3.12 and 3.4.13.	2026-08-25	6.1	CVE-2026-55059
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. Versions prior to 3.2.10, 3.3.12, and 3.4.13 contain an infinite-loop vulnerability in <code>SampleCountChannel</code> . The helper <code>roundListSizeUp()</code> rounds a sample-list size up to the next power of two using repeated unsigned left shifts, which terminates for normal values but fails for <code>UINT_MAX</code> : the sequence reaches <code>0x80000000</code> , and the next left shift wraps the 32-bit value to 0. Because 0 remains less than <code>UINT_MAX</code> , the loop never progresses and never exits. The bug is reachable through public <code>OpenEXRUtil</code> APIs, either by editing the sample-count buffer through <code>SampleCountChannel::Edit</code> (whose destructor calls <code>endEdit()</code>) or by calling <code>SampleCountChannel::set(x, y, UINT_MAX)</code> on a valid pixel. This issue has been fixed in versions 3.2.10, 3.3.12, and 3.4.13.	2026-08-25	6.2	CVE-2026-55373
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. From version 3.4.0 through 3.4.13, a crafted HTJ2K-compressed EXR can crash OpenEXR during normal decode. An HTJ2K-compressed EXR whose JPEG 2000 SIZ fields place the first tile outside the visible image can reach invalid tile and codeblock geometry in the vendored <code>OpenJPH AVX2</code> decoder, causing a stack out-of-bounds write and denial of service. OpenEXR's HTJ2K path validates the decoded codestream dimensions against the EXR chunk size, but it does not reject SIZ image-offset/tile-grid geometry where the first tile does not intersect the image. This issue is fixed in version 3.4.14.	2026-08-24	6.5	CVE-2026-68516
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. In versions 3.1.0 through 3.2.10, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13, an <code>int32_t</code> multiplication in <code>OpenEXRCore's unpack_sample_table()</code> can overflow while decoding a crafted deep tiled EXR file, producing an invalid pointer that leads to a read from an unmapped memory address and a crash. Because the overflow occurs in the standard decoding path (<code>exr_decoding_run</code>), any application that decodes deep tiled EXR files is affected. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	5.5	CVE-2026-59183
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. OpenEXR versions before 3.2.11, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13 are vulnerable on ILP32 builds to an out-of-bounds read. The vulnerability is reached when a crafted uncompressed deep-tile EXR causes the sample-count table size calculation in <code>OpenEXRCore decoding.c</code> to wrap before <code>unpack_sample_table()</code> iterates over the full attacker-controlled tile dimensions, allowing denial of service. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	5.5	CVE-2026-59983
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. OpenEXR versions 3.1.0 through 3.2.10, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13 are vulnerable on ILP32 builds to an out-of-bounds write. When a crafted B44-compressed scanline EXR causes the logical scratch size to truncate before allocation and <code>uncompress_b44_impl()</code> writes using the attacker-controlled channel width,	2026-08-25	5.5	CVE-2026-59984

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allowing denial of service and memory corruption. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.			
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. OpenEXR versions 3.2.0 through 3.2.10, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13 are vulnerable on ILP32 builds to a heap out-of-bounds read. The issue occurs when a crafted RLE-compressed EXR causes the 64-bit unpacked size to truncate before allocation in OpenEXRCORE decoding.c and unpack_32bit() reads beyond the resulting buffer, allowing denial of service. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	5.5	CVE-2026-59985
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. OpenEXR versions before 3.2.11, 3.3.0 through 3.3.12, and 3.4.0 through 3.4.13 are vulnerable to crashing. This occurs when Imf::GetChannelsInMultiPartFile() processes a crafted EXR with an empty multiView header attribute and Imf::viewFromChannelName() indexes the empty vector for a dotless channel name. This issue is fixed in versions 3.2.11, 3.3.13, and 3.4.14.	2026-08-25	5.5	CVE-2026-61555
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image file format, widely used in the motion picture industry. In versions 3.3.0 through 3.3.12 and 3.4.0 through 3.4.13, the PyOpenEXR Python bindings contain a heap out-of-bounds write triggered when reading a crafted deep scanline EXR file. When a deep file declares a literal channel named left alongside layer-prefixed RGB channels left.R, left.G, and left.B, the wrapper processes the literal left channel first and allocates a scalar deep sample array for it, then reuses that same array as the coalesced destination for the prefixed RGB group. The deep reader registers sample slices with an RGB stride (three lanes) into storage that was allocated with scalar shape, so decoding the deep samples writes past the allocation. Opening such a file through the default public Python API, OpenEXR.File(path), causes a heap buffer overflow during normal deep sample decode, leading to memory corruption and a crash. This issue is fixed in versions 3.3.13 and 3.4.14.	2026-08-25	5.5	CVE-2026-68514
AcademySoftware Foundation--openexr	OpenEXR is the reference implementation and specification for the EXR image file format, widely used in the motion picture industry. In versions 3.3.0 through 3.3.12 and 3.4.0 through 3.4.13, the PyOpenEXR Python bindings return stale heap data when reading a crafted deep scanline EXR that uses layer-prefixed RGB channels. With the default channel coalescing (separate_channels=False), the wrapper groups channels such as left.R, left.G, and left.B into a single RGB sample array, but the lane-offset calculation in PyPart::setDeepSliceData() only recognizes the exact unprefixed names G, B, and A. As a result, prefixed channels like left.G and left.B are decoded into lane 0 while lanes 1 and 2 are left uninitialized and returned to Python. A Python application that reads untrusted deep EXR files through the default OpenEXR.File API and then logs, serializes, previews, or otherwise processes the resulting NumPy sample arrays may expose uninitialized same-process heap contents, in addition to receiving incorrect green and blue channel data. This issue is fixed in versions 3.3.13 and 3.4.14.	2026-08-25	4.3	CVE-2026-62986
ACF Extended--ACF Extended	Contributor Broken Access Control in ACF Extended <= 0.9.2.6 versions.	2026-08-28	4.3	CVE-2026-81284
achorein--expo-share-intent	A security flaw has been discovered in achorein expo-share-intent up to 8.0.0. This affects the function getDataColumn of the file ExpoShareIntentModule.kt of the component Android File Copy Routine. The manipulation of the argument _display_name results in path traversal. The attack requires a local approach. Upgrading to version 8.0.1 is able to mitigate this issue. The patch is identified as c6900b1ed06fcc3ca4b09651348974ac5b95e4e6. The affected component should be upgraded.	2026-08-24	4.4	CVE-2026-78196
Admidio--admidio	Admidio versions before 5.0.12 contain a broken access control vulnerability in profile_function.php that allows authenticated low-privilege users to read another	2026-08-30	4.3	CVE-2026-82658

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user's future role memberships. Attackers can bypass profile-level authorization by directly calling the reload_future_memberships endpoint with a victim's user UUID to disclose sensitive membership information.			
Adobe--Adobe DNG Software Development Kit (SDK)	DNG SDK versions 1.7.1 2502 and earlier are affected by an out-of-bounds read vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information from memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-27	5.5	CVE-2026-34616
Adobe--Adobe DNG Software Development Kit (SDK)	DNG SDK versions 1.7.1 2502 and earlier are affected by an out-of-bounds write vulnerability that could lead to application denial-of-service. An attacker could leverage this vulnerability to corrupt memory, causing the application to crash or become unresponsive. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-27	5.5	CVE-2026-34620
Adobe--Adobe Substance 3D Designer	Substance3D - Designer is affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	5.5	CVE-2026-48429
Adobe--C2PA Tool	CAI Content Credentials is affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-25	6.2	CVE-2026-71444
Adobe--C2PA Tool	CAI Content Credentials is affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-08-25	6.2	CVE-2026-76189
Adobe--C2PA Tool	CAI Content Credentials is affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	5.5	CVE-2026-76198
Adobe--Illustrator Desktop 2026	Illustrator is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	5.5	CVE-2026-71441
Adobe--Substance3D - Painter	Substance3D - Painter is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-08-25	5.5	CVE-2026-75752
Ahmad--WP Job Portal	Subscriber Insecure Direct Object References (IDOR) in WP Job Portal <= 2.5.9 versions.	2026-08-28	4.3	CVE-2026-81299
Airtable--airtable-mcp-cli	The configure command accepted any endpoint URL and stored it beside the user's access token. ConfigureCommand.execute in src/cli.ts persisted the value given to its endpoint option into the user profile without passing it through createSafeUrl in src/config.ts, the helper that already restricted the environment-variable form of the same setting to the vendor's own hosts over HTTPS. Because the connect path in src/mcp.ts attaches the stored token as a bearer credential on every request to the configured endpoint, a user who was persuaded to run configure with an endpoint of the attacker's choosing sent their personal access token to that destination on each subsequent invocation. Version 0.2.5 applies the same helper to the option.	2026-08-27	6.5	CVE-2026-81101

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Akilli Ticaret Software Technologies Ltd.--E-Commerce Pack	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Akilli Ticaret Software Technologies Ltd. E-Commerce Pack allows Stored XSS. This issue affects E-Commerce Pack: from 4.5.001 through 28082026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-28	5.4	CVE-2026-4378
AlexGladkov--claude-in-mobile	A security flaw has been discovered in AlexGladkov claude-in-mobile 3.10.2. This affects the function execSync of the file src/adb/client.ts. Performing a manipulation results in os command injection. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. Upgrading to version 3.10.3 is able to mitigate this issue. The patch is named a86d9e55694c98a122943eeff859461d0b9aa6d6. It is suggested to upgrade the affected component.	2026-08-27	5.3	CVE-2026-81562
AnalogWP--Style Kits	Subscriber Broken Access Control in Style Kits <= 2.6.5 versions.	2026-08-24	6.5	CVE-2026-27364
apitable--apitable	APITable through 1.13.0-beta.1 annotates the create handler of InternalNotifyController with requiredLogin = false. ResourceInterceptor honours that annotation by returning before any session or API key is validated, and the nginx gateway shipped with the product proxies every /api request to the backend server, so POST /api/v1/internal/notification/create is reachable by any unauthenticated client that can reach the gateway. An attacker can persist arbitrary notifications in apitable_player_notification against any user ID they name, and because fromUserId can be set to 0 the message is stored with the system sender and renders in the victim's inbox as a legitimate system notification. The body extras content is stored verbatim and forwarded to the frontend.	2026-08-27	5.3	CVE-2026-80207
aquaproj--aqua	aqua is a declarative command-line version manager written in Go. Prior to 2.60.1, pkg/unarchive/archives.go in the handler.HandleFile method calls os.Symlink with archives.FileInfo.LinkTarget without verifying that the target remains under the extraction destination. A later regular-file entry at the same archive path is opened with OpenFile using O_CREATE and O_WRONLY, which follows the attacker-planted symlink. A malicious or compromised package archive can therefore write attacker-controlled bytes outside aqua's extraction directory with the privileges of the user running aqua, potentially overwriting shell startup files, tool configuration, or writable executable paths. This issue is fixed in version 2.60.1.	2026-08-28	6.6	CVE-2026-55569
arben-adm--mcp-sequential-thinking	A vulnerability has been found in arben-adm mcp-sequential-thinking up to 0.5.0. Impacted is the function import_session/export_session of the file mcp_sequential_thinking/server.py of the component Import Session/Export Session. Such manipulation of the argument file_path leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 0.6.0 is recommended to address this issue. The name of the patch is 2fad3ee8ab1d0868b6c1afb5895bc336a10e5267. Upgrading the affected component is recommended.	2026-08-27	6.3	CVE-2026-81845
authlib--joserfc	joserfc is a Python library that provides an implementation of several JSON Object Signing and Encryption (JOSE) standards. Prior to version 1.7.3, JWTClaimsRegistry applies membership matching to list-valued iss and sub claims, allowing an array-valued iss that contains the expected issuer to pass an intended equality check and enabling issuer-validation bypass. This issue is fixed in version 1.7.3.	2026-08-24	6.5	CVE-2026-75509
Autodesk--3ds Max	A maliciously crafted SVG file, when parsed through Autodesk 3ds Max, can trigger an Uncontrolled Recursion vulnerability. A malicious actor may leverage this vulnerability to cause the application to terminate unexpectedly, resulting in a denial-of-service.	2026-08-24	5.5	CVE-2026-16781
Autodesk--3ds Max	A maliciously crafted SVG file, when parsed through Autodesk 3ds Max, can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this	2026-08-24	5.3	CVE-2026-16782

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.			
automatisch--automatisch	Automatisch reveals whether an address is registered through the response to its forgot-password request. The controller at packages/backend/src/controllers/internal/api/v1/users/forgot-password.js looks the address up and chains a not-found throw onto the query, so an address with no account raises an error that the global handler renders as a not-found status, while a registered address proceeds to send the reset message and returns no-content. The route is mounted without authentication. Submitting candidate addresses and comparing the two status codes therefore establishes which addresses hold accounts, with no credential and no rate limiting in the path.	2026-08-26	5.3	CVE-2026-81033
Baserow--Baserow	Baserow interpolates a user's display name into the rich-text mention markup without HTML encoding. PATCH /api/user/account/ stores the first_name value verbatim, and the mention renderer in web-frontend/modules/core/editor/mention.js builds its element with a template literal that places the name into a data-label attribute and the element body unescaped. A name containing a double quote closes that attribute and the opening tag, so following markup lands in the element content. The result is rendered through v-html by the rich-text field components, so any rich-text cell mentioning the account executes the stored script for every workspace member who views the table, without a click. Any workspace member, at the lowest permission level, can set the name and reach every other member of the workspace, and the payload persists until the name is changed or the mentioning row is removed. Version 2.3.0 escapes the value before interpolation.	2026-08-24	6.4	CVE-2026-76837
Beetel--450TC3	A vulnerability was determined in Beetel 450TC3 01.00.00_01. This affects an unknown part. Executing a manipulation can lead to weak password recovery. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-30	6.3	CVE-2026-82487
Bendix--EC80ESP+J1708	Bendix EC80 Brake ECU is vulnerable to an out-of-bounds write, which could allow an attacker to deliver a payload that could establish an arbitrary write primitive, which could crash the ECU.	2026-08-27	6.5	CVE-2026-68967
Bendix--EC80ESP+J1708	Bendix EC80 Brake ECU uses hard-coded credentials, which could allow an attacker to disable automatic traction control.	2026-08-27	5.4	CVE-2026-71396
bentoml--BentoML	BentoML's outbound connection safeguard (make_safe_connect in _internal/utils/uri.py) blocks private, loopback, and link-local IP addresses but fails to reject the RFC 6598 shared address space (100.64.0.0/10, CGNAT). In versions 1.4.19 through 1.4.39, an unauthenticated attacker can supply URLs pointing to that range via multipart file handling (MultipartSerde.ensure_file) or JSON request parsing (JSONSerde.parse_request), causing the server to make outbound requests to internal hosts on CGNAT networks (Server-Side Request Forgery). This is an incomplete fix for CVE-2025-54381.	2026-08-24	5.8	CVE-2026-78205
BilPark Informatics Technologies Industry and Trade Inc.--DoXBASE	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in BilPark Informatics Technologies Industry and Trade Inc. DoXBASE allows Cross Zone Scripting. This issue affects DoXBASE: through 27082026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-27	6.1	CVE-2026-5738
blackms--aistack	A vulnerability was identified in blackms aistack up to 1.6.1. Affected by this issue is some unknown functionality of the file src/web/server.ts of the component Static File Handler. Such manipulation of the argument req.url leads to path traversal. The attack can be executed remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-27	5.3	CVE-2026-81560

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
BookStackApp--BookStack	BookStack before 26.05.4 contains a broken access control vulnerability that allows authenticated API users with image-update or image-delete permissions to manipulate other users' avatars by exploiting missing content-type restrictions in the Image Gallery API endpoints. Attackers can supply a user avatar's ID to the API controller, which loads any image type without the web controller's gallery and drawio restrictions, and when the avatar's uploaded_to field matches a page ID accessible to the attacker, the authorization check passes allowing the attacker to rename, replace, or delete the target user's avatar without requiring user-management permission.	2026-08-24	5.4	CVE-2026-67204
browser-use--web-ui	browser-use web-ui versions 2.0.0 through 3.0.0 fail to validate browser settings paths in run_agent_task, allowing attackers to create directories at arbitrary locations by supplying absolute paths to save_recording_path, save_trace_path, save_agent_history_path, or save_download_path parameters. Attackers can exploit this via the unauthenticated Gradio interface to create directories anywhere the root-running container has write access.	2026-08-30	5.3	CVE-2026-82637
browser-use--web-ui	browser-use web-ui versions 2.0.0 through 3.0.0 write configured LLM API keys to disk in cleartext without encryption or access restrictions. Attackers with read access to the temporary settings directory can recover provider API keys from predictably-named JSON files.	2026-08-30	5.5	CVE-2026-82640
bsmi021--mcp-file-context-server	A vulnerability was detected in bsmi021 mcp-file-context-server 1.0.0. Affected by this issue is the function read_context of the file src/index.ts of the component Path Resolution. Performing a manipulation of the argument path results in path traversal. It is possible to initiate the attack remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-27	5.3	CVE-2026-81486
buildwps--PPWP Password Protect Pages	The PPWP - Password Protect WordPress #1 Most-Reviewed Password Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'ppwp' shortcode in all versions up to, and including, 1.9.21 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-25	6.4	CVE-2025-9878
bytebot-ai--bytebot	A vulnerability was identified in bytebot-ai bytebot 0.0.1. The affected element is an unknown function of the component Agent Execution Workflow. Such manipulation leads to infinite loop. The attack may be performed from remote. The exploit is publicly available and might be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-08-24	4.3	CVE-2026-78250
cakephp--debug_kit	DebugKit provides a debugging toolbar for CakePHP applications. Prior to 4.10.3 and 5.2.4, the DebugKit MailPreview feature in src/Controller/MailPreviewController.php accepts a route-controlled previewName value in findPreview and passes the resolved class from App::className() to constructor execution without rejecting namespace separators or verifying that the class extends DebugKit\Mailer\MailPreview. An attacker able to access DebugKit while debug mode is enabled and the request hostname is local or allowlisted can select an unintended application class through the mail-preview preview route, resulting in arbitrary constructor execution and limited disclosure of application information. This issue is fixed in versions 4.10.3 and 5.2.4.	2026-08-26	4.3	CVE-2026-54614
CAYIN Technology--CAYIN CMS-WS	CAYIN CMS-WS and CMS-SE developed by CAYIN Technology have a Missing Authentication vulnerability. Unauthenticated remote attackers can obtain media file lists via specific functionality, resulting in partial information disclosure.	2026-08-26	5.3	CVE-2026-80234
Ceviz Informatics Inc.--Web Design	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Ceviz Informatics Inc. Web Design allows Reflected XSS. This issue affects Web Design: through 25082026.	2026-08-28	6.1	CVE-2026-5953

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Chainlit--chainlit	Chainlit through 2.12.0 fails to validate ownership of feedback records in PUT and DELETE endpoints. Authenticated attackers can delete or modify other users' feedback by supplying arbitrary feedback identifiers, corrupting human-rating data used for model evaluation.	2026-08-28	5.3	CVE-2026-82290
cockpit-hq--cockpit	Cockpit CMS before 2.14.1 contains an account enumeration vulnerability in the auth check endpoint due to timing discrepancies in password verification. Attackers can measure response times across multiple requests to determine which accounts exist by observing that existing accounts trigger bcrypt verification while non-existent accounts return immediately.	2026-08-29	5.3	CVE-2026-82449
code-projects--Online Shopping System	A vulnerability has been found in code-projects Online Shopping System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/submit_form.php. Such manipulation of the argument Success leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-08-25	4.3	CVE-2026-79793
continew-org--continew-admin	ContiNew Admin fails to apply file-upload permission checks or file-type allowlist validation to multipart upload endpoints, allowing authenticated users to store files with arbitrary extensions. Attackers can initialize chunked uploads, send file parts, and complete uploads to leave arbitrary files in the storage backend accessible via web server URLs.	2026-08-25	6.5	CVE-2026-80050
contrid--Newsletters	The Newsletters plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.17. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with author-level access and above, to send arbitrary newsletter emails to users of any WordPress role, including administrators, by forging POST fields during a normal post submission. This allows an attacker-supplied role slug via the newsletters_mailinglistsroles POST field to be passed directly to get_users(), enabling unauthorized mass-mailing and potential phishing against privileged site users through the site's own outbound email channel.	2026-08-25	4.3	CVE-2026-75908
cozmoslabs--TranslatePress Translate Multilingual sites with AI Translation	The TranslatePress - Translate Multilingual sites with AI Translation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Approved Comment Body Rendered in Translation Editor Strings Dropdown in all versions up to, and including, 3.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-25	6.4	CVE-2026-18512
cozythemes--Cozy Blocks Page Builder for Gutenberg Editor & FSE with 700+ Patterns, 58 Blocks & Templates	The Cozy Blocks - Page Builder for Gutenberg Editor & FSE with 700+ Patterns, 58 Blocks & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via cozyHoverEffect Block Attribute in all versions up to, and including, 2.2.16 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload survives wp_kses_post on save because it contains no angle brackets - only a double-quote breakout of the cozyHoverEffect.boxShadow.color attribute value - allowing event-handler injection at the render stage.	2026-08-25	6.4	CVE-2026-75019
Creativeitem--Ekushey Project Manager CRM	Ekushey Project Manager CRM stores the administrator-configured system name and writes it to the login page without output encoding. The value is emitted in three places on that page: the content attribute of the description meta element, the title element, and the text of an h4 element in the page header. The h4 occurrence is parsed as markup, so HTML placed in the system name field is rendered as markup and any event handler it carries runs. The login page is served without authentication, so the stored value executes in the browser of every visitor who loads it, including visitors who are not signed in, within the origin that serves the login form and alongside the credential fields on it. Storing the value requires	2026-08-25	4.8	CVE-2026-26211

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	an administrator session; the resulting script runs for unauthenticated visitors and persists until the setting is changed.			
CRI-O--CRI-O	A flaw was found in CRI-O's container-creation environment-variable handling ('mergeEnvs' in 'server/utils.go', consumed by 'setupContainerEnvironmentAndWorkdir' in 'server/container_create.go'). When a 'CreateContainer' request supplies a 'nil' CRI 'Envs' field, CRI-O falls back to using the target OCI image's 'config.Env' entries unfiltered, in contrast to the normal merge path, which validates each entry for a 'key=value' form before use. An OCI image whose 'config.Env' contains an entry with no '=' character (e.g. a bare 'NOEQUALS' string) causes CRI-O to split that entry into a single-element slice and then index its second element, which is out of range. This triggers an unrecovered Go runtime panic in the 'crio' daemon process, crashing it and terminating the container-runtime service for all workloads on the node until it is restarted.	2026-08-24	6	CVE-2026-17113
cthackers--adm-zip	adm-zip 0.5.9 through 0.6.0 follows symbolic links at the extraction destination. Utils.sanitize in util/utils.js enforces containment by comparing only the string form of an archive entry name against the resolved extraction root, and Utils.writeFileTo opens the computed destination with fs.openSync(path, "w", 0o666), which resolves symbolic links and carries neither O_NOFOLLOW nor a pre-write fs.lstatSync check. When a path component at the destination already exists as a symbolic link pointing outside the extraction root, extractAllTo, extractAllToAsync and extractEntryTo write the entry contents through that link and then chmod its target, placing attacker-controlled content in a file outside the root without any traversal sequence appearing in the archive. Reaching the write requires overwrite to be enabled, because the preceding fs.existsSync check also resolves the link and otherwise declines. An attacker able to create a symbolic link inside a shared, reused or predictable extraction directory, such as a temporary directory or a continuous integration workspace, can overwrite any file the extracting process is permitted to write.	2026-08-24	6.5	CVE-2026-76845
CVHub520--X-AnyLabeling	X-AnyLabeling's model downloader disabled TLS certificate verification. download_with_retry in anylabeling/services/auto_labeling/model.py built a context with ssl._create_unverified_context() and passed it to urllib.request.urlopen, so neither the certificate chain nor the hostname was checked on any model download, and models are fetched over HTTPS from the project's release host. Any party positioned to intercept that connection could therefore answer it with content of their own choosing. The response is written to a .part file and moved into place with os.replace, and the only post-download check, safe_check_model, validates the file's format rather than its provenance: no hash or signature is compared against an expected value. For an ONNX target the substituted file passes onnx.checker.check_model and is then used for inference, so the attacker chooses the model that produces the application's annotations. For a .pth or .pt target, which the shipped SAM2 video, YOLOE, UPN and open_vision configurations use, the check worker calls torch.load without weights_only, so a substituted file is unpickled and executes code of the attacker's choosing on PyTorch releases predating the weights_only default.	2026-08-25	5.9	CVE-2026-79785
CyberTutor--NewSiteServer (NSS)	NewSiteServer (NSS) developed by CyberTutor has an Arbitrary File Upload vulnerability. Unauthenticated remote attackers can upload arbitrary files, including malicious HTML files, thereby achieving effects similar to cross-site scripting.	2026-08-24	6.1	CVE-2026-19852
CyberTutor--NewSiteServer (NSS)	NewSiteServer (NSS) developed by CyberTutor has a Missing Authentication vulnerability. Unauthenticated remote attackers can exploit a specific functionality to send emails to anyone on behalf of the school.	2026-08-24	5.3	CVE-2026-19853
danielpopamd--linkedin-ads-mcp	A security vulnerability has been detected in danielpopamd linkedin-ads-mcp 1.0.0. Affected by this vulnerability is the function fs.readFileSync of the file src/tools/campaign-management.ts of the component Media Upload. Such manipulation of the argument filePath leads to path traversal. The attack may be	2026-08-27	5.3	CVE-2026-81485

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	performed from remote. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.			
Dayneks Software Industry and Trade Inc.--E-Commerce Platform	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Dayneks Software Industry and Trade Inc. E-Commerce Platform allows Reflected XSS. This issue affects E-Commerce Platform: through 28082026. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-28	6.1	CVE-2026-5800
Dell--Alienware Area 51m R2	Dell Client BIOS contains an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary Write	2026-08-24	6.6	CVE-2026-63693
Dell--Cloud Disaster Recovery	Dell Cloud Disaster Recovery, versions 20.2 and prior, contain a Server-Side Request Forgery (SSRF) vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Server-side request forgery.	2026-08-26	4.3	CVE-2026-71172
Dell--iDRAC9	Dell iDRAC9, 14G versions prior to 7.00.00.182 and 15G/16G versions prior to 7.20.30.50, contains an Improper Access Control vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to gaining access to unauthorized data.	2026-08-26	5.9	CVE-2026-79940
Dell--Power Protect Cyber Recovery	Dell PowerProtect Cyber Recovery, versions 20.2 and prior, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2026-08-26	6.5	CVE-2026-49809
Dell--Power Protect Cyber Recovery	Dell PowerProtect Cyber Recovery, versions Prior to 20.3, contain an UNIX Symbolic Link (Symlink) Following vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Script injection.	2026-08-26	5.8	CVE-2026-79939
Dell--PowerProtect One	Dell PowerProtect One, versions 20.1.0.0 and below, contain an Authorization Bypass Through User-Controlled Key vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information tampering.	2026-08-26	6.5	CVE-2026-74771
Dell--PowerProtect One	Dell PowerProtect One, versions 20.1.0.0 and below, contain a Reliance on Insufficiently Trustworthy Component vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Cache poisoning.	2026-08-26	5.3	CVE-2026-67275
Dell--PowerProtect One	Dell PowerProtect One, versions 20.1.0.0 and below, contain an Improper Certificate Validation vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	2026-08-26	5.9	CVE-2026-74774
designextreme--Reviews and Rating Google Reviews	The Reviews and Rating - Google Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.10. This is due to the wp_display() shortcode handler, used by multiple shortcodes, allowing attacker-controlled html_tags values to define raw HTML tags and then embedding untrusted vicinity content inside those tags. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-26	6.4	CVE-2026-2388
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains a reflected cross-site scripting vulnerability in the extra fields administration template where the type request parameter is echoed without JavaScript-context encoding into an inline script block and no Content-Security-Policy header is emitted. An unauthenticated attacker can cause an authenticated administrator to open a crafted URL to execute arbitrary JavaScript in that session and create a persistent administrator account.	2026-08-24	6.1	CVE-2026-71503

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains a broken object-level authorization vulnerability in the REST API company bank account write routes that allows authenticated attackers with third-party creation rights to create, replace, or delete bank account details of any company without requiring read access to that company. Attackers can inject attacker-controlled IBANs as creditor accounts, which are then written into regenerated SEPA credit-transfer files, redirecting outgoing payments to attacker-controlled accounts.	2026-08-24	6.5	CVE-2026-71507
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains an improper authorization vulnerability in the user REST API update endpoint that allows attackers with user-write rights to modify payroll fields by exploiting an incomplete credential denylist that omits payroll columns. Attackers can rewrite salary, bonus, hourly rate, daily rate, and weekly hours for any user without holding payroll rights, with the modified values appearing in payroll export reports.	2026-08-24	6.5	CVE-2026-71508
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains an improper authorization vulnerability in the expense report REST API update endpoint that allows authenticated attackers with expense-creation rights to bypass the approval workflow by directly setting approval status and approver identity fields. Attackers can manipulate workflow state fields through the REST API to advance expense reports to approved or closed status without possessing the dedicated approval right, while also creating forensic inconsistencies in audit records due to missing approval timestamps.	2026-08-24	6.5	CVE-2026-71509
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains a SQL injection vulnerability in the users REST API that allows authenticated attackers with user-read rights to extract sensitive data by splicing unsanitized filter parameters into SQL WHERE clauses without column restrictions. Attackers can perform binary search on numeric fields and LIKE prefix iteration on string fields to recover salary figures and password verifiers omitted from normal API responses, while raw database error messages in the same endpoint enable column name enumeration.	2026-08-24	6.5	CVE-2026-71510
Dolibarr--dolibarr	Dolibarr before 24.0.0 contains a sensitive data exposure vulnerability in the Members REST API that allows authenticated attackers with member-read rights to retrieve bcrypt password verifiers by querying member endpoints. Attackers can call the individual member or member list endpoints to obtain crypted password verifier fields that are not filtered by the base API serializer or the Members API class, potentially enabling offline password cracking attacks.	2026-08-24	6.5	CVE-2026-71511
Dolibarr--dolibarr	Dolibarr before 23.0.4 authorizes REST API document deletion against the wrong permission. Documents::delete() in htdocs/api/class/api_documents.class.php calls dol_check_secure_access_document() with the mode argument 'read' when handling DELETE /api/index.php/documents, while the sibling builddoc() path passes 'write', the correct mode for an operation that modifies stored data. An authenticated API user who holds only a read permission for a document-bearing module, for example societe:lire or facture:lire, and no create, write, delete or admin permission, therefore passes the check and can permanently delete that module's documents: third-party files, invoices, orders, proposals, project files and generated PDFs, with no recovery path. The call site is htdocs/api/class/api_documents.class.php:1276 in 23.0.3 and passes 'write' from 23.0.4 onward.	2026-08-27	6.5	CVE-2026-81729
Dolibarr--dolibarr	Dolibarr 21.0.0 before 24.0.0 contains an authorization bypass vulnerability caused by an inverted boolean condition in the private-project membership check within the clonetasks mass action handler in htdocs/core/actions_massactions.inc.php. Authenticated users with project creation permission but without access to a target private project can exploit the flawed !in_array() check to clone tasks into unauthorized private projects.	2026-08-24	4.3	CVE-2026-77923
Dolibarr--dolibarr	Dolibarr versions 10.0.0 before 24.0.0 fail to perform per-object authorization checks in the Users::getGroups REST API endpoint, allowing authenticated users to retrieve group memberships of other users. Attackers can call GET	2026-08-30	4.3	CVE-2026-82633

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/users/{id}/groups with arbitrary user identifiers to access group names, entity associations, and private notes across tenant boundaries.			
Dolibarr--ERP	A vulnerability has been found in Dolibarr ERP up to 18.0.10/22.0.5/23.0.3. This issue affects some unknown processing of the file /user/note.php of the component User Notes Handler. The manipulation of the argument ID leads to authorization bypass. The attack can be initiated remotely. Upgrading to version 23.0.4 and 24.0.0 is capable of addressing this issue. The identifier of the patch is 9b5229ef3a9b58d00252d327936b022fb739f149. Upgrading the affected component is advised.	2026-08-24	6.3	CVE-2026-78160
doorkeeper-gem--doorkeeper-openid_connect	Doorkeeper OpenID Connect implements an OpenID Connect authentication provider for Rails applications on top of Doorkeeper. Prior to 1.10.4, the Dynamic Client Registration (DCR) endpoint persists client-supplied scopes without validating them against the server's configured scope set. Under certain conditions, this allows a self-registered client to obtain scopes beyond what the server intended to grant. In DynamicClientRegistrationController#application_params, the scopes attribute is assigned directly from params[:scope] with no validation against Doorkeeper.configuration.scopes or optional_scopes. Combined with enforce_configured_scopes being off by default and Doorkeeper's ScopeChecker prioritizing application-level scopes over server-level scopes, this creates a privilege escalation path. This issue is fixed in version 1.10.4.	2026-08-25	4.2	CVE-2026-70665
DrayTek Corporation--VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a null pointer dereference vulnerability in the formlogout function. The vulnerability is caused by missing checks for an empty or absent Cookie header before string handling. A remote attacker can trigger this vulnerability via a crafted request to crash the service and cause a denial of service. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	4.9	CVE-2026-71920
DrayTek Corporation--VigorSwitch G2540xs	Multiple DrayTek VigorSwitch models contain a directory traversal vulnerability in the getSyslogFile function. The vulnerability is caused by insufficient validation of the option field. A remote attacker can trigger this vulnerability via crafted input containing path traversal sequences to access arbitrary files on the device. Exploitation requires valid administrative credentials for the device's web management interface.	2026-08-24	4.9	CVE-2026-71932
eazsolution--EasyFix	EAZ EasyFix 12.9 allows a Security Feature Bypass related to a "Missing Cryptographic Step" associated with "Secure Boot disable."	2026-08-27	6	CVE-2026-25250
Ebyte--Ebyte NE2-D11 Firmware	The affected Ebyte device web management interface does not restrict the interface from being rendered within an external frame. An unauthenticated remote attacker could use a crafted webpage to mislead an authenticated administrator into initiating unintended configuration changes or disruptive actions.	2026-08-27	5.4	CVE-2026-75548
Ebyte--Ebyte NE2-D11 Firmware	Administrative credentials may be exposed in plaintext within the Ebyte device's management interface, increasing the risk of credential compromise through visual or remote observation. This undermines the confidentiality of device access.	2026-08-27	4.6	CVE-2026-73839
Elastic--Kibana	Authorization Bypass Through User-Controlled Key (CWE-639) in Kibana can lead to unauthorized data modification via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). Under certain conditions, an authenticated user could reference another user's AI Assistant conversation identifier to access or modify a conversation they do not own. Successful exploitation requires knowledge of a hard-to-guess identifier.	2026-08-25	4.2	CVE-2026-78581
elwerene--libreoffice-convert	libreoffice-convert is a Node.js module for converting office documents to different formats. Prior to 1.8.2, index.js uses the caller-controlled options.fileName value in path.join(tempDir.name, fileName) without reducing it to a base name. A filename containing ../ can escape the temporary directory because path.basename() normalization is missing and write the supplied document buffer to an arbitrary	2026-08-27	6.5	CVE-2026-54732

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	path writable by the process, including an SSH authorized_keys file, a cron configuration, or a web root. This issue is fixed in version 1.8.2.			
FasterXML--com.fasterxml.jackson.core:jackson-databind	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. Prior to versions 2.18.9, 2.21.5, 2.22.1, 3.1.5, and 3.2.1 on their respective release lines, the java.net.InetAddress branch of FromStringDeserializer.Std._deserialize() calls InetAddress.getByName() on attacker-controlled input, causing eager DNS resolution during deserialization and enabling DNS-based server-side request forgery and internal-host enumeration. This issue is fixed in versions 2.18.9, 2.21.5, 2.22.1, 3.1.5, and 3.2.1.	2026-08-24	5.3	CVE-2026-77310
Faveo--Helpdesk	A flaw has been found in Faveo Helpdesk up to 2.0.3. This impacts the function FormController::post_ticket_reply of the file app/Http/Controllers/Client/helpdesk/FormController.php of the component post-ticket-reply Endpoint. This manipulation causes missing authentication. The attack can be initiated remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-24	6.5	CVE-2026-78434
filebrowser--filebrowser	filebrowser through 2.63.23 fails to validate named pipes in directory archive and public download handlers, allowing attackers to trigger blocking open syscalls. Authenticated users or anonymous visitors with public share links can repeatedly request archives containing named pipes to pin server goroutines and exhaust connection resources.	2026-08-28	5.9	CVE-2026-82235
FishCodeTech--Muteki	A security vulnerability has been detected in FishCodeTech Muteki up to 0.2.5. The affected element is an unknown function of the file .claude/settings.json of the component Default Local Worker Backend. The manipulation leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The issue was closed with the comment (translated from Chinese): "The project will be refactored and shut down."	2026-08-25	6.3	CVE-2026-79623
fleetdm--fleet	Fleet is an open-source device management platform built on osquery. In versions up to and including 4.84.1, the labels host-listing endpoint (GET /api/v1/fleet/labels/{id}/hosts) allowed an authenticated user with the lowest-privilege Observer role to extract host enrollment secrets through a sort-order oracle. The endpoint accepted a user-supplied order_key parameter that was not validated against a column allowlist, so an attacker with Global or Team Observer access could set the sort column to a sensitive field such as h.node_key and combine it with the cursor-based after parameter to binary-search the value one character at a time; the targeted value never appeared in the response, but the presence or absence of results revealed each character. Because node_key and orbit_node_key are the long-lived shared secrets that osquery and Orbit agents use to authenticate to the Fleet server, an attacker who reconstructed them could impersonate enrolled hosts, submit fabricated query results and inventory, retrieve pending scripts and MDM commands, and poison compliance and policy results across the deployment. This issue is fixed in version 4.84.2.	2026-08-26	6.5	CVE-2026-46370
fleetdm--fleet	Fleet is an open-source device management platform built on osquery. In versions up to and including 4.84.1, the Apple MDM commands listing endpoint (GET /api/v1/fleet/mdm/apple/commands) allowed an authenticated user with the lowest-privilege Observer role to extract sensitive values from joined database tables, including host enrollment secrets and Apple Push Notification Service tokens, through a sort-order oracle. The endpoint accepted a user-supplied order_key parameter that was not validated against a column allowlist, and because the underlying query joins the hosts and nano_enrollments tables, an attacker could set the sort column to a sensitive field and combine it with the cursor-based after parameter to binary-search the value one character at a time, with the presence or absence of results revealing each character even though the value never appeared in the response. With extracted node_key or orbit_node_key values an attacker could impersonate enrolled hosts to Fleet's osquery and Orbit	2026-08-26	6.5	CVE-2026-46371

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	endpoints, submit fabricated host data, and retrieve pending scripts and commands. This issue is fixed in version 4.84.2.			
fleetdm--fleet	Fleet is an open-source device management platform built on osquery. In versions prior to 4.87.0, the target search endpoint (POST /api/latest/fleet/targets) returned unmasked team enroll secrets and full team configuration, including credential-bearing agent options, to low-privilege observer-class users. Other team-facing endpoints mask these fields for observers, but the target search endpoint did not apply the same sanitization, so an authenticated user with the Observer, Observer+, or Technician role, whether global or team-scoped, could retrieve the secrets and agent options by performing a target search against an observer-runnable query. With a leaked team enroll secret an attacker could enroll unauthorized hosts into the affected team, and if the team's agent options contained credentials such as AWS secret access keys or proxy passwords, those values were disclosed as well. This issue is fixed in version 4.87.0.	2026-08-26	6.5	CVE-2026-48786
fleetdm--fleet	Fleet is an open-source device management platform built on osquery. In versions prior to 4.85.0, the global policy read endpoint (GET /api/latest/fleet/policies/{policy_id}) fails to verify team ownership of the requested policy, allowing an authenticated user with observer-level access on any single team to read the full details of policies belonging to any other team and bypass Fleet's team isolation model. The handler authorizes the request against an empty policy object whose TeamID is nil, which an authorization rule permits for any user holding a role on any team, and then fetches the policy by ID with no team filter and returns it without any post-fetch scope check. Because policy IDs are sequential integers, an attacker can enumerate them to read other teams' policy SQL queries, host pass and fail counts, and associated software-installer and script metadata, exposing security-monitoring strategies and compliance posture across team boundaries. This issue is fixed in version 4.85.0.	2026-08-26	4.3	CVE-2026-41262
flextype--flextype	Flextype CMS through v1.0.0-dev contains an expression language injection vulnerability that allows authenticated attackers with a valid API token to read arbitrary files by passing unsanitized user-supplied input to the Symfony ExpressionLanguage engine via the POST /api/v1/query endpoint. Attackers can leverage exposed application objects including filesystem() and serializers() within the evaluation scope to read arbitrary server files and achieve conditional remote code execution if a PHP file can be placed on disk through a secondary vector.	2026-08-28	6.5	CVE-2026-77939
fonoster--fonoster	The updateWorkspace handler in mods/identity/src/workspaces/createUpdateWorkspace.ts in Fonoster through 0.22.7 invokes the gRPC callback with PERMISSION_DENIED when createlsWorkspaceMember reports that the caller is not a member of the target workspace, but it does not return. Execution continues into prisma.workspace.update, which is scoped by the workspace reference alone, so the rename commits before the second callback is issued and the caller receives a permission error for a write that already succeeded. The gRPC interceptor in mods/common/src/identity/createAuthInterceptor.ts binds the workspace accessKeyId to the caller's token only for paths in workspaceResourceAccess or workspaceResourceOwnerOrAdminAccess, and Identity/UpdateWorkspace is listed in fullIdentityAccess, which the base USER role holds. Any authenticated user can therefore rename an arbitrary workspace in the deployment.	2026-08-27	4.3	CVE-2026-80209
Forgejo--Forgejo	A vulnerability was found in Forgejo up to 15.0.4. This issue affects the function net.LookupIP of the file services/migrations/allowlist/is_migrate_allowed.go of the component Repository Migration Handler. Performing a manipulation results in server-side request forgery. The attack can be initiated remotely. The exploit has been made public and could be used. The patch is named b313bb83f5f22bcc0378e0e0ca7bbd58303f168. It is recommended to apply a patch to fix this issue. The project maintainer explains: "I don't intend to backport this to v15 or v16 as it is a breaking change."	2026-08-30	6.3	CVE-2026-82556

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
formulaagile--My Agile Privacy CMP, Cookie Consent & Privacy Tools	The My Agile Privacy CMP, Cookie Consent & Privacy Tools plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.3.6. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to modify plugin settings including missing_cookie_shield, cookie_shield_running, cmode_v2_js_on_error, cmode_v2_js_error_code, and cmode_v2_js_error_motivation stored in the plugin's settings key.	2026-08-25	5.3	CVE-2026-17587
frappe--frappe	Frappe Framework development builds contain an authorization flaw in the render_jinja_template endpoint that allows low-privileged users to render arbitrary Jinja templates by supplying raw template strings. Attackers with print permission on any document can execute arbitrary SELECT statements against unrelated tables, including reading password hashes from the __Auth table.	2026-08-30	6.5	CVE-2026-82634
frappe--frappe	Frappe 15.11.0 through 16.32.0 stores and renders the workspace card description without XSS filtering. The description field of the Workspace Link doctype is declared with "ignore_xss_filter": 1 in frappe/desk/doctype/workspace_link/workspace_link.json, and _sanitize_content() in frappe/model/base_document.py skips any field carrying that flag, so the value is stored exactly as submitted. frappe.desk.desktop.get_desktop_page returns it unchanged, and LinksWidget.set_body() in frappe/public/js/frappe/widgets/links_widget.js interpolates it into a Bootstrap popover created with html: true, by way of the __() translation helper, which performs no HTML escaping. A user holding the Workspace Manager role can therefore place arbitrary markup in a public workspace's card description and have it execute in the session of any desk user who opens that workspace and hovers the description, including higher-privileged users, allowing session token theft and authenticated requests as the victim. The flag is removed on the development branch but remains present in the shipped 15.x and 16.x release lines, so no released version carries the fix.	2026-08-27	5.4	CVE-2026-81731
FrontAccounting--FrontAccounting	FrontAccounting through 2.4.20 generates a CSRF token in end_form() in includes/ui/ui_controls.inc and embeds it as the _token hidden field in every form it renders, but only admin/users.php and admin/change_current_user_password.php call check_csrf_token() to validate it. No financial transaction handler validates the token, including gl/gl_journal.php, gl/gl_bank.php, purchasing/supplier_invoice.php, sales/customer_invoice.php, sales/customer_payments.php and admin/company_preferences.php, so those endpoints act on POST data with no origin check. An attacker who gets an authenticated user to load a page under attacker control can auto-submit a cross-origin form to any of them and have the forged journal entry, invoice, customer payment, bank transaction or company configuration change recorded under the victim's session.	2026-08-27	6.5	CVE-2026-80210
FrontAccounting--FrontAccounting	FrontAccounting through 2.4.20 stores and verifies user passwords as unsalted MD5 digests. admin/users.php passes md5(\$_POST['password']) to add_user() and update_user_password(), admin/change_current_user_password.php does the same when a user changes their own password, the forgotten-password path in includes/current_user.inc hashes the newly generated password the same way, and authentication calls get_user_auth(\$loginname, md5(\$password)). The codebase applies no per-password salt and contains no call to password_hash(), password_verify() or any other adaptive hash, so identical passwords yield identical digests and an attacker who obtains the user table can recover plaintext passwords with precomputed lookup tables or high-rate GPU cracking.	2026-08-27	5.9	CVE-2026-80211
getformwork--Formwork	Formwork through 2.3.14 contains a stored cross-site scripting vulnerability in visit tracking that records the Referer header host unescaped. Unauthenticated attackers can craft malicious Referer headers to inject markup that executes in administrator browsers when viewing the Statistics panel.	2026-08-29	6.1	CVE-2026-82451

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getgrav--grav	Grav CMS before 2.0.16 contains a path traversal vulnerability in the media_directory() Twig function that fails to validate filesystem paths, allowing authenticated users to enumerate and access files outside intended scope. Attackers with page authoring privileges can supply arbitrary filesystem paths to media_directory() and use the allow-listed filepath accessor on Medium objects to read file contents of any file matching configured media extensions that the web server process can access.	2026-08-25	6.5	CVE-2026-72697
getgrav--grav	Grav CMS before 2.0.16 fails to filter system, site, and theme configuration arrays in sandboxed Twig renders, allowing content editors to read sensitive configuration values. Attackers with page-content edit access can access raw configuration arrays including secrets like cache credentials by using dot notation in Twig templates, bypassing the config_denied_paths restrictions.	2026-08-25	6.5	CVE-2026-72698
getgrav--grav	Grav before 2.0.16 allows sandboxed Twig templates to access sensitive User fields through allow-listed offsetGet() and offsetexists() methods that lack field filtering. Attackers with page-edit permissions can call offsetGet() on User objects to extract hashed passwords and 2FA secrets, enabling offline password cracking and authentication bypass.	2026-08-25	6.5	CVE-2026-76839
getgrav--grav	Grav API plugin before 1.0.16 contains a server-side request forgery vulnerability in webhook delivery that allows attackers to bypass hostname validation by DNS rebinding. Attackers controlling authoritative DNS for a configured webhook hostname can answer validation lookups with public addresses and delivery lookups with private addresses to reach internal network resources.	2026-08-25	5.3	CVE-2026-56708
getgrav--grav	Grav CMS before 2.0.16 contains an origin validation bypass in the Uri::referrer() and Pages::referrerRoute() methods, which validate the Referer header using an unanchored string prefix match (str_starts_with(\$referrer, \$base)) with no trailing delimiter. An attacker who controls a domain that begins with the victim site's origin (e.g. https://example.com.attacker.tld) can send a request with such a Referer to be treated as same-origin, bypassing the Referer-based origin check.	2026-08-25	5.4	CVE-2026-72702
getgrav--grav	The Grav API plugin (getgrav/grav-plugin-api) before 1.0.18 does not apply the API-key scope cap in the injectSecurityTab() function of BlueprintController when deciding whether a page's security/permissions blueprint section is editable. Because the function performs raw isSuperAdmin()/hasPermission() checks without a request parameter, it cannot enforce scopeAllows(). A caller holding a scoped API key may therefore see (and potentially edit) page permission fields beyond the scope granted to the key. The end-to-end write-time impact was not fully confirmed by the reporter.	2026-08-26	5.4	CVE-2026-80204
getgrav--grav-plugin-login	The Grav Login plugin (getgrav/grav-plugin-login) before 3.9.1 is vulnerable to email address enumeration. The register() method in classes/Login.php throws a distinct exception (EMAIL_NOT_AVAILABLE) when a submitted email address already belongs to an existing account, while allowing registration to proceed otherwise. Because the registration endpoint has no rate limiting, an attacker can enumerate which email addresses have accounts on the site, one guess per request.	2026-08-25	5.3	CVE-2026-72699
GhostManager--Ghostwriter	Ghostwriter through 7.2.6 does not apply per-object authorization on its report template lint endpoints. RoleBasedAccessControlMixin.test_func returns only request.user.is_active unless a view overrides it, and neither the endpoint that lints a report template nor the endpoint that returns stored lint results provides an override, so each resolves a ReportTemplate from a caller-supplied primary key with no ownership or client-scope check. Any authenticated account can therefore lint an arbitrary template, which overwrites that template's stored lint result, and can read the returned findings, which enumerate the template's variable names and template-engine errors and so disclose its structure. This is distinct from the template swap path: that endpoint authorizes the report but omits the per-	2026-08-24	5.4	CVE-2026-78204

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	template check, whereas these endpoints omit authorization entirely and remain unfixed.			
gilbertchen--duplicacy	Duplicacy through 3.2.5 contains a path traversal vulnerability in the restore function that fails to validate entry paths deserialized from snapshot files. Attackers can craft malicious snapshot entries with directory traversal sequences to write files outside the restore directory to arbitrary locations accessible by the restoring user.	2026-08-28	6.8	CVE-2026-82264
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 11.10 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user could have caused denial of service, due to an unbounded loop triggered by specially crafted input in the SCIM user provisioning feature.	2026-08-26	6.5	CVE-2025-10903
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.8 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, could have allowed an authenticated user to cause a denial of service affecting background job processing, due to missing object count limits.	2026-08-26	6.5	CVE-2026-77801
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 11.3 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user with project Maintainer permissions could have accessed the terminal of a protected environment they were not authorized to use due to improper authorization checks.	2026-08-26	5.5	CVE-2026-3035
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 18.3 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user could have assigned compliance frameworks from namespaces they were not authorized to access to their own project, due to missing namespace validation on self-managed instances.	2026-08-27	5.4	CVE-2026-4398
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.7, 19.2 before 19.2.5, and 19.3 before 19.3.1 that, under certain conditions, an authenticated user with developer-role permissions could have influenced the execution environment of Pipeline Execution Policy enforcement jobs, due to improper handling of job dependencies.	2026-08-26	4.3	CVE-2026-15387
GitoxideLabs--gitoxide	gitoxide gix-packetline versions before 0.21.5 contain a panic vulnerability in the TextRef implementation that occurs when processing side-band packet lines with empty payloads. A malicious Git server can send a crafted side-band packet to trigger an index out of bounds panic, aborting the client process during fetch operations without authentication.	2026-08-28	6.5	CVE-2026-82250
GitoxideLabs--gitoxide	gitoxide versions from 0.25.4 contain an HTTP credential leak vulnerability in the curl-based transport backend where credentials are sent to attacker-controlled servers after HTTP redirects. The vulnerability occurs because credential validation checks the original URL instead of the effective URL after redirect, allowing attackers to steal authentication tokens through cross-domain redirects or HTTPS-to-HTTP downgrades.	2026-08-28	6.8	CVE-2026-82255
GitoxideLabs--gitoxide	gix-worktree-state before 0.33.0 (part of gitoxide) allows writing files outside the worktree on Windows. gix_worktree_state::checkout() follows an existing terminal symlink during non-exclusive (incremental) materialization (destination_is_initially_empty: false) when core.symlinks is true. If a symlink entry (mode 120000) is first checked out at a path P pointing outside the worktree, a subsequent incremental checkout of a regular-file entry (mode 100644) at the same path follows the existing reparse point and writes the blob content through the link, overwriting files outside the worktree.	2026-08-28	5.3	CVE-2026-82248

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitpython-developers--GitPython	GitPython versions before 3.1.59 contain an incomplete denylist in the <code>unsafe_git_revision_options</code> guard that omits <code>--contents</code> and <code>-S</code> options, allowing attackers to read arbitrary files by passing these options to <code>Repo.blame()</code> . Attackers can supply revision values like <code>--contents=/etc/passwd</code> to leak file contents through the blame result returned to the caller.	2026-08-25	6.5	CVE-2026-78678
gitpython-developers--GitPython	GitPython before 3.1.59 contains an arbitrary file read vulnerability in <code>TagReference.create()</code> where a positional reference parameter bypasses the <code>unsafe</code> option guard. Attackers can supply a reference value like <code>--file=<path></code> to read arbitrary files, with contents returned in the annotated tag message.	2026-08-25	6.5	CVE-2026-78679
GNOME--GIMP	A flaw was found in the file-pix (ESM) plugin in GIMP. When processing a specially crafted PIX image file, the plugin allocates a Variable-Length Array (VLA) on the stack without proper bounds checking, causing an unbounded stack allocation followed by a 21-byte stack over-read. This can result in a denial of service due to stack exhaustion and a limited information disclosure of stack memory contents into an intermediate file.	2026-08-24	6.1	CVE-2026-78475
GNOME--GIMP	A flaw was found in the Seattle FilmWorks plugin in GIMP. When processing a specially crafted SFW image file, the plugin allocates a Variable-Length Array (VLA) on the stack without integer overflow checks, causing an unbounded stack allocation. This issue leads to an application crash, resulting in a denial of service.	2026-08-26	5.5	CVE-2026-79902
GNOME--GIMP	A flaw was found in the file-xwd plugin in GIMP. When processing a specially crafted XWD image file, the plugin validates the image width and bytes-per-line parameters independently rather than ensuring their combined values are consistent with the allocated buffer size. This incorrect validation leads to improper bounds checking, causing a heap out-of-bounds read. This issue can result in an application crash, leading to a denial of service, or a limited information disclosure of heap memory contents into the produced image.	2026-08-25	4.4	CVE-2026-80101
go-vikunja--vikunja	Vikunja is an open-source self-hosted task management platform. Prior to 2.4.0, <code>POST /api/v1/projects/{project}/views/{view}/buckets/{bucket}</code> allows the request body <code>project_view_id</code> value to be mass assigned by <code>Bucket.Update</code> in <code>pkg/models/kanban.go</code> . The permission check validates that the bucket currently belongs to the URL project and view but does not validate the body selected destination view, allowing any authenticated user to relocate an attacker-owned bucket into another tenant's Kanban view. The injected bucket retains attacker-controlled content and ownership, enabling cross-tenant defacement. This issue is fixed in version 2.4.0.	2026-08-28	5	CVE-2026-55067
go-vikunja--vikunja	Vikunja is an open-source self-hosted task management platform. From 2.3.0 until 2.4.0, a user with Write but not Admin permission on a shared child project can detach it from its parent hierarchy by submitting <code>parent_project_id</code> equal to 0 to <code>POST /api/v1/projects/{project}</code> . The <code>Project.CanUpdate</code> authorization check in <code>pkg/models/project_permissions.go</code> and <code>UpdateProject</code> logic in <code>pkg/models/project.go</code> only gate nonzero parent values, while <code>UpdateProject</code> always persists <code>parent_project_id</code> , so the explicit zero value bypasses the Admin requirement introduced for CVE-2026-35595. Detachment severs the recursive permission-inheritance chain and can disrupt the owner's hierarchy and inherited collaborator access. This issue is fixed in version 2.4.0.	2026-08-28	4.3	CVE-2026-55064
gohugoio--hugo	Hugo's default fenced-code-block renderer writes attribute values taken from the code-fence info string into the rendered HTML without escaping them. New in <code>markup/internal/attributes/attributes.go</code> converts every attribute value from a byte slice to a string as it is stored, deliberately dropping the escaping that used to happen there, and <code>RenderAttributes</code> in the same file escapes only values that are still byte slices, so its escaping branch is never reached and every value is written verbatim. The function's documentation states that it performs HTML escaping of string attributes, which it does not. A quote inside an attribute value in the info string therefore terminates the attribute and allows a further attribute, including	2026-08-24	5.4	CVE-2026-10618

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	an event handler, to be placed on the wrapper element, and the script runs for every visitor who loads the page. This path is reached under the default configuration, with code fences enabled and without goldmark's unsafe setting or any custom render hook. Attribute names beginning with on are filtered when the attributes are parsed, so injection is achieved through the value rather than the name.			
GOVCERT-LU--eml_parser	eml_parser serves as a python module for parsing eml files and returning various information found in the e-mail as well as computed information. Prior to 3.0.2, the clean_found_uri function in eml_parser/parser.py validates potential URL strings before unescaping HTML entities used for colon, slash, or period characters. Valid encoded URLs and their host names are therefore rejected and omitted from the extracted URL and domain lists. Email security gateways and SOC pipelines that use those lists as indicators of compromise may fail to submit the hidden URLs to threat intelligence feeds, reputation services, or sandboxes, allowing malicious links to bypass inspection. This issue is fixed in version 3.0.2.	2026-08-25	6.5	CVE-2026-55618
GOVCERT-LU--eml_parser	eml_parser serves as a python module for parsing eml files and returning various information found in the e-mail as well as computed information. Prior to 3.0.2, eml_parser.parser.HeaderParser.header_fetch_parse in eml_parser/parser.py uses email.utils.getaddresses() to parse address-bearing e-mail headers. A deeply nested CFWS comment construct exhausts the standard-library recursive descent parser's call stack and raises RecursionError, which is not caught and therefore aborts parsing of the entire message. An attacker can disrupt SOC pipelines that process untrusted EML files, although callers already need to handle exceptions from malformed or pathological messages. This issue is fixed in version 3.0.2.	2026-08-25	5.3	CVE-2026-55619
Grafana--Clickhouse Datasource	When the ClickHouse plugin uses Native protocol (the default) with PDC or secure SOCKS, it asks for TLS but the connection library ignores that and talks to ClickHouse in the clear. Username, password, queries, and results can be read on the hop after the proxy. The server certificate is never checked, and a configured client certificate is not sent.	2026-08-27	6.1	CVE-2026-19854
Grafana--Grafana OSS	An authenticated attacker with Editor access or alert.instances.external:write can submit an external Alertmanager alert containing a controlled generatorURL. The attacker is authorized to create the alert, but not to execute script in another user's Grafana session. Grafana renders alert.generatorURL directly as the Alert Details See source LinkButton href without URL-scheme sanitization or a safe-protocol allowlist. The click interceptor's :// heuristic can be bypassed by placing :// inside a JavaScript comment. When a user with read access clicks See source, the browser executes attacker-controlled JavaScript in the Grafana origin with the clicking user's permissions.	2026-08-24	6.8	CVE-2026-17033
Grafana--Grafana OSS	A user with organization administrator permissions can delete dashboard snapshots belonging to other organizations on the same Grafana instance, and can recover a snapshot's secret delete key using only its public share key (broken access control).	2026-08-26	6.3	CVE-2026-19197
gravitl--netmaker	Netmaker disables certificate verification on the connection to the configured mail server. The sender in pro/email/smtp.go assigns a TLS configuration whose skip-verify field is set to true unconditionally, directly beneath a comment stating that the setting should be false in production. No configuration value governs it and no code path restores verification, so the client accepts any certificate the mail server presents, including one an interposing party supplies. Mail that Netmaker sends over that connection includes password-reset messages carrying single-use tokens and user invitations carrying enrolment links, so a party positioned on the path between the server and its mail relay can read those messages in transit and use a captured reset token before the intended recipient does. The setting is absent from the development branch but present in the latest release.	2026-08-26	6.5	CVE-2026-81034

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Graylog2--graylog2-server	Graylog is a free and open log management platform. From 7.1.0 until 7.1.4 and 7.2.0-alpha.2, the System Catalog entity titles endpoint in graylog2-server/src/main/java/org/graylog2/rest/resources/system/contentpacks/titles/EntityTitleServiceImpl.java allows an authenticated user to request composite display fields without verifying that every selected field is readable. A user can retrieve protected values, including the password hash on a readable user record; ordinary users are limited to their own permitted records, while administrators can retrieve hashes for all users. This issue is fixed in versions 7.1.4 and 7.2.0-alpha.2.	2026-08-28	5	CVE-2026-55425
hank-ai--darknet	darknet subscribes its layer array with an index taken from a configuration file without checking it against the array's length. The array is allocated in src-lib/darknet_network.cpp as xmalloc(net.n, sizeof(Darknet::Layer)), sized to exactly the number of layer sections the file declares. The shortcut, scale_channels and sam sections supply that index through their from field and the route section through its layers field, and parse_shortcut_section in src-lib/darknet_cfg.cpp reads net.layers[index].outputs with no bounds check, which reads past the allocation. The dispatch loop in create_network then reuses the same index to assign net.layers[l.index].use_bin_output and net.layers[l.index].keep_delta_gpu, writing past the allocation at an offset the file controls, with a fixed one-byte value. Parsing a crafted configuration file is sufficient: the parse runs before any weights file is opened and needs no non-default option, so the result is a reliable crash and a write whose location, though not its value, is chosen by whoever supplied the file.	2026-08-27	6.1	CVE-2026-81334
HashiCorp--Vault	A vulnerability was identified in HashiCorp Vault and Vault Enterprise ("Vault") such that an authenticated attacker may manipulate an identity value referenced by a templated policy path to gain unintended access to Vault paths. An attacker who can control the referenced identity value may include slash ({{/}}) characters that Vault interprets as additional path segments when rendering the policy. This vulnerability, CVE-2026-5006, was fixed in Vault Community Edition 2.0.4 and Vault Enterprise 2.0.4, 1.21.9, 1.20.14, and 1.19.20.	2026-08-24	6.8	CVE-2026-5006
HashThemes--Hash Form	Unauthenticated Cross Site Request Forgery (CSRF) in Hash Form <= 1.4.0 versions.	2026-08-24	4.3	CVE-2026-78280
hatchet-dev--hatchet	Hatchet is a platform for orchestrating background tasks, AI agents, and durable workflows at scale. From 0.40.0 until 0.91.1, the Dispatcher gRPC service does not verify that a request's worker ID belongs to the tenant identified by the bearer-token context in Dispatcher/UpsertWorkerLabels and Dispatcher/Unsubscribe. An authenticated owner of any tenant who guesses another tenant's worker UUID can overwrite that worker's affinity labels or disconnect the worker from the dispatcher. This can cause cross-tenant integrity impact and denial of service on multi-tenant Hatchet Cloud or shared self-hosted deployments. Single-tenant deployments are not practically affected because the attacker and target tenant are the same. This issue is fixed in version 0.91.1.	2026-08-28	6.4	CVE-2026-54746
HCL Software--Hive	HCL Hive is affected by multiple infrastructure and network configuration vulnerabilities, which could lead to unauthorized lateral movement, container breakout, and sensitive data exposure within internal communications.	2026-08-25	5.4	CVE-2026-21754
HCL Software--Hive	HCL Hive is affected by weak software supply chain governance, which could lead to the inclusion of vulnerable, unmaintained, or malicious third-party dependencies within the application environment.	2026-08-25	4.2	CVE-2026-21753
HCL Software--IEM	HCL IntelliOps Event Management (IEM) is affected by a Session Deletion Vulnerability. It may allow improper handling of user sessions, resulting in sessions not being fully terminated after logout or deletion.	2026-08-27	6.4	CVE-2025-62342
HCLSoftware--BigFix Quantum Risk Analyzer	HCL BigFix Quantum Risk Analyzer generates highly detailed logging information by default which increases the risk of sensitive data leakage and can provide an attacker with internal application logic and architectural details.	2026-08-26	4.1	CVE-2026-21808

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
HCLSoftware--BigFix Quantum Risk Analyzer	HCL BigFix Quantum Risk Analyzer is affected by a hardcoded external resource reference and a lack of binary integrity which could allow an attacker to obtain sensitive information or modify the binary.	2026-08-26	4.4	CVE-2026-21810
HCLSoftware--HCL Hive	HCL Hive Keycloak IAM Instance is affected by insufficient granularity of access control which could allow an attacker unauthorized access to resources.	2026-08-24	5.3	CVE-2025-68833
HCLSoftware--HCL Hive	HCL Hive is affected by a missing rate limit which could allow an attacker unauthorized access via brute-force or credential stuffing attacks, or cause a denial of service.	2026-08-24	5.3	CVE-2026-21755
HCLSoftware--HCL Hive	HCL Hive is affected by an information exposure vulnerability where Swagger documentation was found exposed publicly. Although no sensitive information (e.g., credentials, PII) was discovered, exposing API documentation to unauthenticated users can increase the overall attack surface.	2026-08-24	4.3	CVE-2026-21759
hookandhook--WP Courses LMS Online Courses Builder, eLearning Courses, Courses Solution, Education Courses	The WP Courses LMS - Online Courses Builder, eLearning Courses, Courses Solution, Education Courses plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.2.29 via the 'resultID' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with custom-level access and above, to read any other user's quiz answers and scores by enumerating the incrementing resultID value via the wpcq_get_quiz_result AJAX action. The only access control on this endpoint is a nonce check (wpc_nonce) that is exposed to every logged-in user on the frontend, providing no meaningful authorization barrier.	2026-08-25	4.3	CVE-2026-10630
horde--imp	Horde IMP's AppleDouble MIME viewer writes an attacker-controlled attachment name into an HTML status block without escaping it. In lib/Mime/Viewer/AppleDOUBLE.php, _IMPRender() obtains the name of the data part with IMP_Contents::getPartName(), which returns the MIME part's own name parameter as supplied by the message, and passes it through sprintf into the text of an IMP_Mime_Status object. IMP_Mime_Status::__toString() concatenates each text entry directly into the surrounding table markup, so the value reaches the rendered page verbatim. A message crafted as multipart/appleDOUBLE whose data part carries markup in its name parameter therefore executes script in the context of any user who views it, and the payload persists in the mailbox. Exploitation requires no account on the target system, only the ability to send mail to a user. Version 7.2.0 escapes the value with htmlspecialchars(). The researcher additionally chains this flaw with the arbitrary file read of CVE-2026-58451, and reports that script running in an administrator's session can reach an application code-execution path.	2026-08-24	6.1	CVE-2026-65053
IBM--Cloud Pak for Data System	IBM Cloud Pak for Data System 11.3.0.2 through Interim Fix 001 is vulnerable to a denial of service due to improper limitation of resources.	2026-08-28	6.2	CVE-2026-3686
IBM--Concert	IBM Concert 1.0.0 through 2.3.1 could allow a remote attacker to perform unauthorized actions using man in the middle techniques due to improper certificate validation.	2026-08-28	5.9	CVE-2025-64649
IBM--Integrated Analytics System	IBM Integrated Analytics System 1.0.0.0 through 1.0.31.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2026-08-28	5.9	CVE-2025-36271
IBM--Integrated Analytics System	IBM Integrated Analytics System 1.0.0.0 through 1.0.31.0 does not validate or improperly validates TLS certificate validation, which could allow an attacker to obtain sensitive information using man in the middle techniques.	2026-08-28	5.9	CVE-2025-36290
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.11.1 could allow a remote authenticated attacker to execute and read any user's private flow due to improper authorization.	2026-08-28	6.4	CVE-2026-19294

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.11.1 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2026-08-28	4.3	CVE-2026-18545
IGEL--IGEL OS 12	IGEL OS 12 before 12.9.0, 12.8.3 LTS and IGEL OS 11 before 11.11.150 contain a secure boot bypass vulnerability in the GRUB boot stage that allows physically present attackers to gain unauthorized root access by placing an unsigned empty file named igel.conf on a partition. Attackers can exploit GRUB's fail-open signature verification behavior to drop into an interactive GRUB prompt, then boot the device's own kernel with additional command-line arguments to obtain a root shell with the disk unlocked while leaving TPM PCR values unaltered.	2026-08-28	6.1	CVE-2026-82018
ilya-zlobintsev--LACT	UNIX symbolic link (symlink) following vulnerability in ilya-zlobintsev/LACT allows for local denial-of-service. This issue affects LACT: through 0.10.0.	2026-08-25	6.1	CVE-2026-75038
immich-app--immich	Immich through 3.1.0 fails to properly enforce locked asset visibility when assets are locked through the single-asset endpoint, allowing them to remain accessible through shared albums and links. Attackers can read locked assets and their metadata by accessing existing shared albums or links, bypassing the locked visibility protection.	2026-08-28	6.5	CVE-2026-82272
implecode--eCommerce Product Catalog	The eCommerce Product Catalog plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'style' Shortcode Attribute in all versions up to, and including, 3.5.10 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload bypasses WordPress's save-time wp_kses_post sanitization because the malicious content is stored inside shortcode brackets with no HTML tags; the tainted HTML output is only generated at render time by the shortcode handler.	2026-08-25	6.4	CVE-2026-76128
iswalle--getnote-mcp	A vulnerability was detected in iswalle getnote-mcp up to 1.5.0. The affected element is the function fs.readFileSync of the file src/index.ts of the component upload_image. Performing a manipulation of the argument image_path results in path traversal. The attack can be initiated remotely. The exploit is now public and may be used. Upgrading to version 1.5.1 is sufficient to fix this issue. The patch is named 7f9a215e03575c650d38c8f87fc6d8d363fed80d. Upgrading the affected component is advised.	2026-08-28	4.3	CVE-2026-82111
itsourcecode--Library Management System	A flaw has been found in itsourcecode Library Management System 1.0. The affected element is an unknown function of the file editbooks.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	2026-08-24	6.3	CVE-2026-78200
itsourcecode--Sales and Inventory System	A vulnerability was detected in itsourcecode Sales and Inventory System 1.0. The impacted element is an unknown function of the file /pages/cust_edit.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	2026-08-24	6.3	CVE-2026-78185
itsourcecode--Sales and Inventory System	A vulnerability was found in itsourcecode Sales and Inventory System 1.0. Affected is an unknown function of the file /pages/cust_del.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	2026-08-25	6.3	CVE-2026-78656
itsourcecode--Sales and Inventory System	A vulnerability was identified in itsourcecode Sales and Inventory System 1.0. This issue affects some unknown processing of the file /pages/emp_edit.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-08-29	6.3	CVE-2026-82421

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itsourcecode--Sales and Inventory System	A security flaw has been discovered in itsourcecode Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/emp_del.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-08-29	6.3	CVE-2026-82422
itsourcecode--Sales and Inventory System	A flaw has been found in itsourcecode Sales and Inventory System 1.0. Affected is an unknown function of the file /pages/emp_searchfrm.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2026-08-30	6.3	CVE-2026-82484
itsourcecode--Sales and Inventory System	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/pro_edit.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-08-30	6.3	CVE-2026-82485
itsourcecode--Sales and Inventory System	A vulnerability was identified in itsourcecode Sales and Inventory System 1.0. Affected is an unknown function of the file /pages/cust_searchfrm.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	2026-08-30	6.3	CVE-2026-82540
itsourcecode--Sales and Inventory System	A security flaw has been discovered in itsourcecode Sales and Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /pages/sup_edit.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	2026-08-30	6.3	CVE-2026-82541
itsourcecode--Sales and Inventory System	A vulnerability has been found in itsourcecode Sales and Inventory System 1.0. Impacted is an unknown function of the file /pages/sup_searchfrm.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2026-08-30	6.3	CVE-2026-82545
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.9 contain an insecure file permissions vulnerability in the desktop GUI that writes decrypted plaintext with world-readable default permissions. Attackers can read decrypted output files created by the GUI as unprivileged local users on multi-user systems.	2026-08-27	6.2	CVE-2026-81682
jahlikes--openssl_encrypt	In openssl_encrypt (pip package openssl-encrypt) versions <= 1.4.8, the desktop GUI passes the steganography password to the CLI child process on the command line via the --stego-password argument (on both encrypt and decrypt paths) instead of via an environment variable as done for the main password. Any local user can read the steganography password from /proc/<pid>/cmdline for the lifetime of the subprocess. Fixed in 1.4.9.	2026-08-27	6.2	CVE-2026-81684
jahlikes--openssl_encrypt	openssl_encrypt 1.4.x before 1.4.9 contains an optional D-Bus crypto service whose org.freedesktop.DBus.Properties.Set method performs neither a polkit authorization check nor value validation. Any local user on the system bus can call Set without authorization and set MaxConcurrentOperations (to 0/negative, causing the concurrency gate to refuse all subsequent operations, or to a huge value removing the limit) or the unbounded DefaultTimeout, resulting in a persistent denial of service of the root daemon. The D-Bus service exists only on the 1.4.x line and was removed in 1.5.x.	2026-08-27	6.2	CVE-2026-81686
jahlikes--openssl_encrypt	openssl_encrypt before 1.4.9 fails to prevent namespace collisions between own identities and contacts in IdentityStore, allowing attackers to create shadowed contact entries invisible until the corresponding own identity is deleted. When the own identity is deleted, the shadowed contact becomes visible and resolves to the attacker's keys, enabling silent key substitution for encrypted files.	2026-08-27	6.8	CVE-2026-81706

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jahlikes-- openssl_encrypt	openssl_encrypt before 1.4.9 fails to validate the memory_cost parameter from identity file protection blocks, allowing attackers to trigger out-of-memory conditions during key derivation. Attackers with write access to local identity stores can craft malicious identity files with excessive memory_cost values that cause the host to crash when unlocking identities before authentication.	2026-08-27	6.2	CVE-2026-81720
jahlikes-- openssl_encrypt	openssl_encrypt versions before 1.4.9 fail to enforce a time ceiling on key derivation function iteration counts specified in file metadata. Attackers can craft files with extremely high KDF iteration counts to consume CPU resources for unbounded periods before password verification occurs.	2026-08-27	5.5	CVE-2026-81687
jahlikes-- openssl_encrypt	openssl_encrypt (pip package openssl-encrypt) versions <= 1.4.8 contain a CWD-relative configuration file resolution flaw in crypt_settings.py, where CONFIG_FILE (originally the absolute per-user path ~/.crypt_settings.json) is reassigned at line 84 to the bare relative name 'crypt_settings.json'. As a result, the legacy Tk GUI's SettingsTab reads and writes KDF settings from crypt_settings.json in the process launch (current working) directory instead of the user's home directory. An attacker who plants a malicious crypt_settings.json (e.g. sha256:1 with all memory-hard KDFs disabled) can silently downgrade encryption performed in that GUI session to roughly one hash round, bypassing the weak-KDF preflight and enabling offline brute-force attacks against the resulting ciphertext. Fixed in 1.4.9.	2026-08-27	5.5	CVE-2026-81697
jahlikes-- openssl_encrypt	openssl_encrypt versions before 1.4.9 fail to validate encryption status of embedded post-quantum private keys in file metadata. Attackers can craft files with unencrypted embedded PQC keys that decrypt under any password, bypassing authentication and producing attacker-chosen plaintext with false integrity verification.	2026-08-27	5.5	CVE-2026-81703
jahlikes-- openssl_encrypt	openssl_encrypt (pip: openssl-encrypt) versions before 1.4.9 contain a path traversal flaw in PluginSandbox._is_safe_path, which authorized file access using a bare string-prefix match. A sandboxed plugin without the READ_FILES permission could read or write another plugin's directory that merely shares a name prefix (e.g., .../plugins/foobar matching allowed .../plugins/foo), breaking per-plugin isolation within the same user. Fixed by matching each allowed directory exactly or with a trailing path separator.	2026-08-27	5.2	CVE-2026-81716
jahlikes-- openssl_encrypt	openssl_encrypt versions before 1.4.9 fail to authenticate recovery-slot presence in envelope-format encrypted files, allowing attackers to remove recovery slots without re-encrypting the payload. Attackers can modify the file header to delete recovery-slot fields and bypass authentication, silently removing recovery paths the owner deliberately added.	2026-08-27	4	CVE-2026-81680
jahlikes-- openssl_encrypt	openssl_encrypt (pip package openssl-encrypt) versions <= 1.4.8 advertise a portable USB workspace as an 'Encrypted USB Workspace' with AES-256-GCM encryption and write a marker declaring the workspace encrypted, but the workspace directory is actually stored in cleartext and the derived encryption key is never applied to it. A user who trusts the branding and places files in the workspace leaves them unencrypted on the removable media, so an attacker with physical access to the media can read the sensitive files. Fixed in 1.4.9, which seals the workspace into an authenticated AES-256-GCM vault.	2026-08-27	4.6	CVE-2026-81681
jegstudio-- Gutenberg WordPress Blocks, Page Builder & Site Editor	The Gutenverse - WordPress Blocks, Page Builder & Site Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'titleTag' Block Attribute in all versions up to, and including, 4.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The malicious titleTag value survives wp_kses_post on save because it is stored inside a block-comment delimiter and the live HTML is only synthesized at render time by do_blocks(), meaning the payload also fires in administrator and editor sessions during post preview.	2026-08-25	6.4	CVE-2026-19943

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jegstudio--Gutenverse WordPress Blocks, Page Builder & Site Editor	The Gutenverse - Ultimate WordPress FSE Blocks Addons & Ecosystem plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the multiple blocks in all versions up to, and including, 4.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-26	6.4	CVE-2026-3002
jeremyevans--rodauth	Rodauth before 2.47.0 contains an authentication bypass vulnerability in the jwt_refresh route that issues new JWT access tokens without requiring a refresh token. Attackers can present an access token to the refresh route via non-POST methods to obtain a new valid access token, enabling indefinite account access with temporary token possession.	2026-08-29	5.4	CVE-2026-82469
jeremyevans--rodauth	Rodauth before 2.47.0 contains a time-based one-time password reuse vulnerability in the otp feature that fails to track the last accepted code timestamp. Attackers who observe a valid TOTP code can replay it during the drift window to bypass the second authentication factor.	2026-08-29	5.4	CVE-2026-82470
jeremyevans--rodauth	Rodauth before 2.47.0 fails to validate protocol-relative return-to paths in confirm_password, login_return_to_requested_location, and two_factor_auth_return_to_requested_location features. Attackers can craft paths with leading double slashes that browsers resolve as protocol-relative URLs, redirecting authenticated users to attacker-controlled sites after login or password confirmation.	2026-08-29	4.7	CVE-2026-82467
jeremyevans--rodauth	Rodauth before 2.47.0 contains a cross-site request forgery protection bypass vulnerability in the JSON request content type validation. Attackers can craft cross-origin form posts with content types containing application/json substrings to bypass CSRF token validation and force victims to authenticate to attacker-controlled accounts.	2026-08-29	4.7	CVE-2026-82468
jfrog--artifactory	An authorization weakness in JFrog Artifactory Composer repository handling may allow an authenticated user, under specific conditions, to read package metadata from repositories they are not authorized to read. The issue affects confidentiality and has been addressed in fixed Artifactory versions.	2026-08-25	6.5	CVE-2026-70550
jowilf--starlette-admin	Starlette-Admin is a fast, beautiful and extensible administrative interface framework for FastAPI and Starlette applications. Prior to 0.16.1, the list API does not validate user-supplied order_by and structured where field names against the configured sortable_fields and searchable_fields allowlists. An authenticated user with access to an affected list endpoint can submit arbitrary field names to starlette_admin/base.py and the BaseModelView validation path, bypassing restrictions presented by the administrative user interface. Requests can sort or filter on fields that are not intended to be sortable or searchable, causing limited information exposure. Invalid field names and special Python attribute names such as metadata and the class dunder attribute can also trigger unhandled exceptions and HTTP 500 responses, causing limited denial of service for targeted requests. This issue is fixed in version 0.16.1.	2026-08-26	5.4	CVE-2026-54553
kimai--kimai	Kimai before 2.63.0 contains a business logic / improper authorization vulnerability in the team update API endpoint (PATCH /api/teams/{id}), which removes all existing team members before validating the submitted replacement member list. An authenticated teamlead (or other user) with permission to edit a team can submit a malformed members payload; although Kimai returns a validation error, the existing membership rows have already been deleted. This bypasses the dedicated member-removal endpoint's protection against removing teamleaders and can leave a team with no members or teamleaders, disrupting team-based access control.	2026-08-25	5.4	CVE-2026-80195
kimai--kimai	Kimai before 2.64.0 contains a missing authorization vulnerability in the ProjectViewController export route (report_project_view_export). The	2026-08-25	4.3	CVE-2026-80194

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authorization guards are attached to the sibling __invoke method rather than at the class level, so the export route inherits no authorization checks. Any authenticated user, including a plain ROLE_USER without the project_reporting permission, can download the project overview export - which returns the same dataset as the protected report - disclosing customer names, project names, currency, budget type, and aggregate totals across all customers. Actual financial figures remain protected in the export template.			
kimai--kimai	Kimai before 2.57.0 contains an improper authorization vulnerability in the favorite timesheet add and remove endpoints that allows authenticated users to manipulate other users' bookmarks. Attackers can add or remove timesheet entries from another user's favorite list by referencing their timesheet identifier, enabling cross-user business-state tampering without administrative privileges.	2026-08-25	4.3	CVE-2026-80197
kimai--kimai	Kimai before 2.53.0 contains an open redirect vulnerability in the SAML authentication success handler that accepts unvalidated RelayState POST parameters as redirect destinations. Attackers with IdP access can supply malicious RelayState values to redirect authenticated users to attacker-controlled URLs for credential theft or phishing attacks.	2026-08-25	4.7	CVE-2026-80200
Le-yan--Medical Practice Management System	Medical Practice Management System developed by Le-yan has a Sensitive Data in URL vulnerability. Unauthenticated remote attackers can obtain sensitive information via victim's browser history or log files.	2026-08-28	5.5	CVE-2026-82181
leanprover--lean4	The Lean 4 kernel does not check that the body of an opaque declaration is closed. environment::add_opaque omits the check_no_metavar_no_fvar call that the definition and theorem paths perform, so a value containing a free variable that is absent from the local context is not rejected outright. A metaprogram can first cause the kernel to create a temporary local of type False and record its type in the type checker's inference cache, then restore the local context while that cache entry persists on the same type checker instance, and finally submit an opaque declaration whose value is the now-unbound variable. The cache lookup answers before the branch that would test membership of the local context, so the kernel infers the cached type and admits an opaque constant of type False, from which any proposition follows. The declaration is accepted through the ordinary checked path at maximum kernel checking, without sorry, unsafeCast, debug.skipKernelTC, addDeclWithoutChecking, foreign code or a modified .olean file, and the result carries no axioms. Fixed in 4.32.2 by adding the missing closure check.	2026-08-24	6.3	CVE-2026-72711
librenms--librenms	LibreNMS is a network monitoring system. In versions up to and including 26.4.0, the Proxmox application view is vulnerable to reflected cross-site scripting through the user-supplied instance and vmid GET parameters, which are reflected into the page title without adequate encoding. The parameters are placed into the page title with only strip_tags applied, and the title is then written into an inline document.title assignment through string interpolation, so a single quote terminates the JavaScript string and the remaining input runs as script. An attacker who lures an authenticated user into following a crafted link can execute script in that user's session, enabling actions such as theft of session data. This issue is fixed in version 26.5.0.	2026-08-26	5.4	CVE-2026-45694
liketrek--TREK	A vulnerability was found in liketrek TREK up to 3.0.22. Impacted is the function loginUser of the file server/src/services/authService.ts of the component Pre-2FA mfa_token Handler. The manipulation results in improper authentication. The attack may be performed from remote. Upgrading to version 3.1.0 is recommended to address this issue. Upgrading the affected component is recommended.	2026-08-25	6.3	CVE-2026-78863
liketrek--TREK	A vulnerability was determined in liketrek TREK up to 3.0.22. The affected element is the function journeyService.updateEntry of the file server/src/nest/journey/journey.controller.t of the component Journey Entry	2026-08-25	6.3	CVE-2026-78864

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Update. This manipulation causes sql injection. It is possible to initiate the attack remotely. Upgrading to version 3.1.0 is sufficient to fix this issue. It is recommended to upgrade the affected component.			
liketrek--TREK	A vulnerability was identified in liketrek TREK up to 3.0.22. The impacted element is the function findOrCreateUser of the file server/src/services/oidcService.ts of the component OIDC Service. Such manipulation leads to improper authentication. It is possible to launch the attack remotely. The attack requires a high level of complexity. The exploitability is regarded as difficult. Upgrading to version 3.1.0 is sufficient to resolve this issue. Upgrading the affected component is advised.	2026-08-25	5.6	CVE-2026-78885
lin-snow--Echo	Ech0 through 4.5.6 registers the PUT /api/echo/like/:id endpoint on the public router group without authentication or rate limiting. Unauthenticated attackers can increment the fav_count counter of any echo (including private echoes) by supplying its UUID, which can be harvested from the public GET /api/echo/page feed. Repeated requests are accepted without deduplication, each triggering a database write and a four-key cache invalidation, allowing attackers to inflate popularity metrics and amplify load on the database and cache. Fixed in 4.7.3.	2026-08-25	6.5	CVE-2026-79661
lin-snow--Echo	Ech0 before 4.4.3 fails to enforce administrator authorization on dashboard log endpoints, allowing any authenticated user to access system logs. Attackers with valid user sessions can query GET /api/system/logs and subscribe to SSE and WebSocket log streams to retrieve sensitive operational data including file paths, stack traces, and internal URLs.	2026-08-25	6.5	CVE-2026-79666
lin-snow--Echo	Ech0 before 4.4.3 protects the PUT /user endpoint with the profile:read scope, a read-only scope, but allows write operations including password changes. An attacker with an admin's profile:read access token can change the admin's password and login to obtain an unrestricted session token that bypasses all scope enforcement.	2026-08-25	6.5	CVE-2026-79673
lin-snow--Echo	Ech0 versions before 4.7.3 expose guest commenter email addresses through public API endpoints due to improper JSON serialization tags on the Comment model. Unauthenticated attackers can harvest all commenter emails by calling the /api/comments and /api/comments/public endpoints without authentication.	2026-08-25	5.3	CVE-2026-79660
lin-snow--Echo	Ech0 before 4.7.3 contains an authentication bypass vulnerability in the PUT /api/echo/like/:id endpoint that allows unauthenticated attackers to increment engagement metrics without identity verification or rate limiting. Attackers can send repeated requests to arbitrarily inflate the fav_count field for any known echo identifier, compromising the integrity of engagement metrics and social ranking systems.	2026-08-25	5.3	CVE-2026-79668
lin-snow--Echo	Ech0 before 4.4.3 contains a server-side request forgery vulnerability in the validateWebhookURL function (webhook_setting_service.go), which only validates literal IP addresses via net.ParseIP() and fails to reject hostnames that DNS-resolve to private or internal IPs (e.g., 169.254.169.254.nip.io). An attacker with admin privileges can create a webhook with such a hostname to bypass validation and cause the server to make requests to internal services, cloud metadata endpoints, and private network resources. The issue is fixed in 4.4.3.	2026-08-25	5.5	CVE-2026-79671
lin-snow--Echo	Ech0 before 4.4.3 fails to enforce scope-based authorization on nine comment panel admin endpoints, allowing access tokens with minimal scopes to perform full comment moderation operations. Attackers with a limited-scope access token can list, approve, reject, delete comments, and modify comment system settings by directly accessing the unprotected panel endpoints.	2026-08-25	5.5	CVE-2026-79672
lin-snow--Echo	Ech0 before 4.7.3 contains a stored cross-site scripting vulnerability in the public RSS feed where tag names and markdown content are rendered without HTML escaping. Attackers with admin privileges can inject malicious tag names or raw	2026-08-25	4.8	CVE-2026-79663

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTML in echo content that executes as JavaScript in RSS readers that render HTML-type summaries, affecting anonymous subscribers and other users.			
lin-snow--Echo0	Ech0 before 4.4.3 lacks authorization checks on system log endpoints allowing any authenticated non-admin user to read and stream all server logs. Attackers can access historical logs and real-time log streams via GET /api/system/logs, GET /api/system/logs/stream, and WS /ws/system/logs to gather reconnaissance data including internal file paths, error stack traces, and application state.	2026-08-25	4.3	CVE-2026-79669
lin-snow--Echo0	Ech0 before 4.4.3 contains a stored cross-site scripting vulnerability in the file upload endpoint that validates Content-Type using only client-supplied headers without server-side inspection. Attackers with admin privileges can upload SVG or HTML files containing JavaScript that executes in the application origin when accessed by any user, enabling session hijacking and data exfiltration.	2026-08-25	4.8	CVE-2026-79670
Linux Foundation--Magma	A vulnerability was found in Linux Foundation Magma 1.9.0. The affected element is an unknown function of the file tasks/amf/amf_fsm.cpp of the component Registration Complete Message Handler. The manipulation results in improper authentication. The attack can be launched remotely. The exploit has been made public and could be used.	2026-08-30	6.5	CVE-2026-82547
Linux Foundation--Magma	A vulnerability was determined in Linux Foundation Magma 1.9.0. The impacted element is an unknown function of the component InitialUEMessage Handler. This manipulation causes information disclosure. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-08-30	5.3	CVE-2026-82548
Linux Foundation--Magma	A security flaw has been discovered in Linux Foundation Magma 1.9.0. This impacts an unknown function of the component NGSetupRequest Handler. Performing a manipulation of the argument NG-IoT-DefaultPagingDRX results in improper input validation. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-30	5.3	CVE-2026-82550
Linux Foundation--Magma	A weakness has been identified in Linux Foundation Magma 1.9.0. Affected is an unknown function of the file ngap_amf_handlers.c of the component NGSetup Handler. Executing a manipulation can lead to state issue. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-30	5.3	CVE-2026-82551
Linux Foundation--Magma	A security vulnerability has been detected in Linux Foundation Magma 1.9.0. Affected by this vulnerability is an unknown functionality of the file tasks/ngap/ngap_amf.c of the component gNB Termination Handler. The manipulation leads to denial of service. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	2026-08-30	4.3	CVE-2026-82552
litespeedtech--LiteSpeed Cache	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via crafted `<img>` tag attributes in all versions up to, and including, 7.7. This is due to a flawed regular expression that is used to strip `width` and `height` attributes from images when the "Lazy Load Images" and "Add Missing Sizes" features are enabled. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that execute whenever a user accesses an injected page.	2026-08-28	6.4	CVE-2026-3129
ljharb--qs	#### Summary `qs.stringify` throws a `TypeError` when it serializes an object whose own `constructor` property has a truthy, non-callable `isBuffer` member. `utils.isBuffer` duck-types buffers by calling `obj.constructor.isBuffer(obj)` after checking only that the property is truthy, so a value such as `{ constructor: { isBuffer: "x" } }` makes the call throw `TypeError: obj.constructor.isBuffer is not a function`. #### Details `lib/stringify.js:127` calls `utils.isBuffer` on every non-primitive value it serializes. `utils.isBuffer` (`lib/utils.js:332`) reads `obj.constructor.isBuffer` and invokes it without verifying that it is a function. `constructor` and `isBuffer` are ordinary property names, so any object carrying	2026-08-29	5.3	CVE-2026-82417

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	them as own properties reaches the unchecked call. Such an object can be built from untrusted input. `qs.parse("x[constructor][isBuffer]=y", { plainObjects: true })` or `{ allowPrototypes: true }` keeps the `constructor` key as an own property (the default parse options drop it), and `JSON.parse("{\"a\":{\"constructor\":{\"isBuffer\":{\"x\"}}})` produces the same shape with no qs option involved. Express 4 with its default `query parser` setting and body-parser with `extended: true` both call `qs.parse` with `allowPrototypes: true`, so on those stacks `req.query` and `req.body` can carry the shape directly. #### PoC ```js var qs = require("qs"); qs.stringify(qs.parse("x[constructor][isBuffer]=y", { plainObjects: true })); qs.stringify(JSON.parse("{\"a\":{\"constructor\":{\"isBuffer\":{\"x\"}}})"); // TypeError: obj.constructor.isBuffer is not a function // at Object.isBuffer (lib/utls.js:332:78) // at stringify (lib/stringify.js:127:45) ``` #### Fix `lib/utls.js`, applied in e83d321 on `main` and released as v6.16.0: ```diff - return !!(obj.constructor && obj.constructor.isBuffer && obj.constructor.isBuffer(obj)); + return !(obj.constructor && typeof obj.constructor.isBuffer === "function" && obj.constructor.isBuffer(obj)); ``` Real `Buffer`, `safer-buffer`, and browserify `buffer` polyfill instances serialize exactly as before; only the throw is removed. ### Affected versions `>=2.2.5 <6.16.0`, fixed in v6.16.0. The unguarded duck-type was introduced in 3768a75 and first shipped in v2.2.5 (September 2014). v2.2.4 and earlier used `Buffer.isBuffer` and are not affected. Every release from v2.2.5 through v6.15.3 contains the unguarded call. ### Impact An unauthenticated request can make any code path that re-serializes attacker-influenced data with `qs.stringify` (for example, rebuilding a query string from `req.query` for a redirect or an upstream request, or serializing a parsed JSON body) throw synchronously. In a typical Node.js HTTP framework the throw is caught by the framework error boundary and the affected request returns a 500; the process survives and other requests are unaffected. Where the call runs outside an error boundary, such as an `async` Express 4 handler (where the throw becomes an unhandled promise rejection) or a background job, the process exits, so the impact in that case depends on the application error handling rather than on qs.			
LogNet--grpc-spring-boot-starter	A vulnerability has been found in LogNet grpc-spring-boot-starter up to 5.2.0. Affected is an unknown function of the component Annotation Processing. Such manipulation leads to improper authorization. The attack may be performed from remote. A high complexity level is associated with this attack. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-30	5	CVE-2026-82594
logto-io--logto	Logto through 1.42.0 contains a server-side request forgery vulnerability in the POST /api/hooks/:id/test endpoint that accepts arbitrary URLs without host validation. Tenant administrators with Management API tokens can make the server issue HTTP POST requests to internal URLs and retrieve response bodies from services on the private network.	2026-08-28	6.8	CVE-2026-82262
logto-io--logto	Logto through 1.42.0 contains a server-side request forgery vulnerability in the OIDC SSO connector creation endpoint that fails to validate the issuer URL parameter. Tenant administrators with Management API credentials can supply arbitrary internal URLs to trigger HTTP GET requests to private network services, with response content returned in API responses.	2026-08-28	6.8	CVE-2026-82263
MAA-AI--MaaMCP	A vulnerability was found in MAA-AI MaaMCP up to 1.1.1.dev6+g2e4a41287. The affected element is the function save_pipeline/load_pipeline of the file pipeline_tools.py. Performing a manipulation results in path traversal. The attack can be initiated remotely. The exploit has been made public and could be used. The patch is named c93ef45cba75295eba26d9ff1ffb9202a91c6150. To fix this issue, it is recommended to deploy a patch.	2026-08-27	5.5	CVE-2026-81847
macrozheng--mall	A vulnerability has been found in macrozheng mall up to 1.0.3. The affected element is an unknown function of the file /order/paySuccess of the component	2026-08-29	5.4	CVE-2026-82423

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Payment Status Endpoint. The manipulation of the argument orderId leads to enforcement of behavioral workflow. The attack is possible to be carried out remotely. The vendor deleted the GitHub issue for this vulnerability without any explanation.			
macrozheng--mall	A security vulnerability has been detected in macrozheng mall up to 1.0.3. Affected is the function OmsCartItemServiceImpl.updateQuantity of the file /cart/update/quantity. The manipulation of the argument quantity leads to business logic errors. The attack may be initiated remotely. The vendor deleted the GitHub issue for this vulnerability without any explanation.	2026-08-25	4.3	CVE-2026-79406
macrozheng--mall	A security vulnerability has been detected in macrozheng mall up to 1.0.3. This impacts an unknown function of the file /order/submit of the component Order Submission. The manipulation leads to race condition. It is possible to initiate the attack remotely. The attack is considered to have high complexity. The exploitability is said to be difficult. The vendor deleted the GitHub issue for this vulnerability without and explanation.	2026-08-29	4.2	CVE-2026-82364
mage-ai--mage-ai	Mage AI does not confine the paths accepted by its browser-items API to the project directory. BrowserItemResource in mage_ai/api/resources/BrowserItemResource.py passes a caller-supplied path to the filesystem read and write helpers without calling the containment helper that the sibling FileContentResource and FileResource classes both use, so the resource contains no such call while those two contain several. A user holding the Viewer role, which grants read access within the project and nothing outside it, can therefore read any file the server process can read by supplying an absolute path. The permission model that would otherwise separate roles is not consulted for this route in the default configuration, because the setting that enables it defaults to false. Callers holding the Editor role additionally write through the same unconfined path, though that role is already able to execute code by design, so the boundary crossed by this flaw is the read available to the Viewer role.	2026-08-26	6.5	CVE-2026-81030
Magepeople inc.--Booking and Rental Manager	Unauthenticated Broken Access Control in Booking and Rental Manager <= 2.7.5 versions.	2026-08-24	5.3	CVE-2026-78258
Magepeople inc.--WpEvently	Contributor Broken Access Control in WpEvently <= 5.5.0 versions.	2026-08-28	5.4	CVE-2026-81759
Magepeople inc.--WpEvently	Subscriber Broken Access Control in WpEvently <= 5.5.0 versions.	2026-08-28	4.3	CVE-2026-81761
mariadb-corporation--mariadb-connector-j	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. Prior to 2.7.14, 3.3.5, 3.4.3, and 3.5.9, when a Java application connects with sslMode=verify-full or sslMode=verify-ca, supplies a password, and does not configure serverSslCert or trustStore, Connector/J can accept an untrusted self-signed certificate through the fallbackToSystemTrustStore=true ephemeral trust manager and record its certFingerprint for later identity binding. The OK-packet and authentication-switch paths enforce the certificate fingerprint, but the initial-handshake path does not. HandshakeResponse.encode() can therefore build and send a mysql_clear_password response before checking certFingerprint != null && !isMitMProof(), sslMode, or whether the authentication plugin is resistant to a man-in-the-middle, and the initial path also bypasses restrictedAuth. An active man-in-the-middle or hostile server can present a self-signed certificate, claim to be MariaDB, select mysql_clear_password as the initial authentication plugin, and receive the full database password before the connection is rejected. This issue is fixed in versions 2.7.14, 3.3.5, 3.4.3, and 3.5.9.	2026-08-28	5.9	CVE-2026-55856
mariadb-corporation--	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. Prior to 2.7.14, 3.3.5, 3.4.3, and 3.5.9, PAM dialog	2026-08-28	5.9	CVE-2026-55857

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mariadb-connector-j	authentication can be coerced into transmitting the account password over an insecure connection. The mysql_clear_password plugin is gated behind a secure transport, but the sibling PAM handler SendPamAuthPacketFactory, named dialog by the server, does not declare that requirement and inherits the default secure-required value false; older branches implement the same affected behavior in SendPamAuthPacket. A hostile or man-in-the-middle server can send an Authentication Switch Request for dialog over plain TCP, causing the driver to return the user's password in cleartext when sslMode=DISABLE and restrictedAuth=null, which is the default configuration. Properly verified TLS and local Unix sockets are not exposed to this transport vector. This issue is fixed in versions 2.7.14, 3.3.5, 3.4.3, and 3.5.9.			
mariadb-corporation--mariadb-connector-j	MariaDB Connector/J is used to connect applications developed in Java to MariaDB and MySQL databases. Prior to 2.7.14, 3.3.5, 3.4.3, and 3.5.9, the connector encodes and decodes protocol text and performs client-side escaping under the assumption that the connection character set is UTF-8. The server can report a mid-session change to character_set_client through OK-packet session-state tracking, including a change caused by SET NAMES, a stored routine or trigger, server configuration, or a hostile server. If character_set_client changes to a non-UTF-8 value, the driver continues to read and write UTF-8 while the server interprets the same bytes under another encoding, causing silent data corruption and a client/server charset-confusion mismatch that can defeat byte-wise quoting or escaping. The fix accepts only utf8, utf8mb3, or utf8mb4 after initialization; any other value causes SQLException with SQLState 08000 and closes the connection. This issue is fixed in versions 2.7.14, 3.3.5, 3.4.3, and 3.5.9.	2026-08-28	5.9	CVE-2026-55858
mariadb-corporation--mariadb-connector-nodejs	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. Prior to 3.2.4, 3.3.3, 3.4.6, and 3.5.3, MariaDB Connector/Node.js permits SQL injection when attacker-controlled Buffer parameters are escaped client-side under the big5, gbk, sjis, cp932, or gb18030 client character sets. PacketOutputStream.writeBufferEscape in lib/io/packet-output-stream.js escaped bytes without the charset-aware getMbRecognizer logic in lib/misc/charset-mb.js. The server SQL lexer runs my_ismbchar before escape processing, so an attacker-controlled lead byte can consume the inserted 0x5C backslash as a multibyte trail byte and leave the following 0x27 quote unescaped, terminating the string literal and allowing arbitrary SQL. The default utf8mb4 character set and parameters sent through the execute binary prepared-statement path are not affected. Successful exploitation can expose or modify data available to the database account. This issue is fixed in versions 3.2.4, 3.3.3, 3.4.6, and 3.5.3.	2026-08-28	6.5	CVE-2026-55855
mariadb-corporation--mariadb-connector-nodejs	MariaDB Connector/Node.js is used to connect applications developed on Node.js to MariaDB and MySQL databases. Prior to 3.2.4, 3.3.3, 3.4.6, and 3.5.3, MariaDB Connector/Node.js can disclose an account password when PAM dialog authentication is negotiated over an insecure transport. In lib/cmd/handshake/auth/pam-password-auth.js and lib/cmd/handshake/authentication.js, the SendPamAuthPacketFactory behavior for the server-side plugin dialog lacked the secure-transport gate applied to mysql_clear_password. With the default sslMode=DISABLE and restrictedAuth=null settings, a hostile or on-path server can send an Authentication Switch Request for dialog over plain TCP, causing the connector to return the account password in cleartext. Properly verified TLS and a local Unix socket prevent this path, while fingerprint-only server identity validation is not sufficient. This issue is fixed in versions 3.2.4, 3.3.3, 3.4.6, and 3.5.3.	2026-08-28	5.9	CVE-2026-55854
mariadb-corporation--mariadb-connector-r2dbc	MariaDB Connector/R2DBC is a non-blocking MariaDB and MySQL client implemented in Java. Prior to 1.4.1, org.mariadb:r2dbc-mariadb encodes and decodes all character data under the assumption that the connection character set is UTF-8. A server can announce a mid-session change to character_set_client through the OK-packet session-state-tracking mechanism, including through SET NAMES executed by a stored routine or trigger, server configuration, or a hostile or	2026-08-28	5.9	CVE-2026-55859

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	man-in-the-middle server. If the new character set is not UTF-8, the driver continues to exchange UTF-8 while the server interprets the same bytes under a different encoding, causing silent data corruption and a client/server charset-confusion mismatch that can defeat byte-wise quoting or escaping. The fix accepts only utf8, utf8mb3, or utf8mb4 after initialization; any other value raises R2dbcNonTransientResourceException with SQLState 08000 and closes the connection. This issue is fixed in version 1.4.1.			
mariadb-corporation--mariadb-connector-r2dbc	MariaDB Connector/R2DBC is a non-blocking MariaDB and MySQL client implemented in Java. Prior to 1.4.1, org.mariadb:r2dbc-mariadb does not gate clear-text password authentication plugins on transport encryption because the AuthenticationPlugin interface has no capability for a plugin to require a secure connection. A hostile or man-in-the-middle MariaDB server can send an AuthSwitchRequest naming mysql_clear_password or dialog (PAM) over a plain-TCP unencrypted connection, and AuthenticationFlow permits ClearPasswordPluginFlow or PamPluginFlow to return the user's password as cleartext bytes on the wire. The disclosed credentials can subsequently be used to authenticate directly to the database server. This issue is fixed in version 1.4.1.	2026-08-28	5.9	CVE-2026-55860
mark3labs--mcp-go	mcp-go accepted requests on its HTTP transports without checking the Host header. StreamableHTTPServer.ServeHTTP in server/streamable_http.go and SSEServer.ServeHTTP in server/sse.go served any request arriving over a loopback connection regardless of the host it named, and the SSE transport's cross-origin default allowed any origin. A page in a browser could therefore point a name it controlled at the loopback address and reach a server listening there, invoking tools and reading resources that the server exposed on the assumption that only local software could connect. No release before 0.56.0 validated the header on either transport; 0.56.0 adds server/http_localhost.go, which rejects a loopback-bound request carrying a host that is not a loopback name, and wires it into both transports.	2026-08-27	6.8	CVE-2026-81092
mastra-ai--mastra	Mastra through 1.63.0 contains an authentication bypass vulnerability in the memory API thread ownership validation when mapUserToResourceId callback is omitted from configuration. Authenticated attackers can enumerate all threads via GET /api/memory/threads and read conversation history and metadata of other resource owners.	2026-08-28	6.5	CVE-2026-82273
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.58, the MCP HTTP Stream _validate_origin method accepts request_origin.startswith(allowed), so the attacker-controlled localhost.evil.example HTTP origin matches the localhost allowlist. Without an API key, a malicious webpage can submit tools/call requests to the local MCP server and execute exposed tools. This issue is fixed in version 4.6.58.	2026-08-25	6.9	CVE-2026-55529
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonaiagents 1.6.58, ast_grep_rewrite lacks the @require_approval decorator used by sibling mutation tools. With dry_run=False, an agent-controlled call can pass --update-all and a broad path to rewrite matching files without the expected authorization gate. This issue is fixed in version 1.6.58.	2026-08-25	6.1	CVE-2026-55530
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.58, the MCP HTTP Stream mcp_post handler creates a new _sessions entry for every initialize request but does not call _cleanup_sessions or enforce a maximum. An unauthenticated caller can exhaust memory. The fix invokes cleanup and limits sessions through PRAISONAI_MCP_MAX_SESSIONS. This issue is fixed in version 4.6.58.	2026-08-25	6.5	CVE-2026-55531
MervinPraison--PraisonAI	PraisonAI is a multi-agent teams system. Prior to praisonai 4.6.58, the Jobs API validate_webhook_url() path fails open on socket.gaierror and does not bind the validated address to the later request. An attacker webhook_url can later resolve to 127.0.0.1, 169.254.169.254, or another internal address. This issue is fixed in version 4.6.58.	2026-08-25	6.8	CVE-2026-55535

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
metaphorcreations--Ditty	Subscriber Broken Access Control in Ditty <= 3.1.67 versions.	2026-08-27	5.3	CVE-2026-81274
Microsoft--Microsoft Edge (Chromium-based)	External control of file name or path in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-08-28	6.5	CVE-2026-66324
Microsoft--Microsoft Edge (Chromium-based)	Incorrect authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2026-08-28	5.4	CVE-2026-62904
Microsoft--Microsoft Edge (Chromium-based)	Improper neutralization of parameter/argument delimiters in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-08-28	5.4	CVE-2026-66323
Microsoft--Microsoft Edge (Chromium-based)	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	2026-08-28	5.4	CVE-2026-70309
Microsoft--Microsoft Edge (Chromium-based)	Improper neutralization of input used for llm prompting in Microsoft Edge for iOS allows an unauthorized attacker to perform spoofing over a network.	2026-08-28	5.4	CVE-2026-70331
Microsoft--Microsoft Edge (Chromium-based)	Concurrent execution using shared resource with improper synchronization ('race condition') in Copilot Chat (Microsoft Edge) allows an authorized attacker to disclose information over a network.	2026-08-28	4.4	CVE-2026-58616
Microsoft--Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-08-28	4.3	CVE-2026-66798
MITRE--Heimdall	In MITRE SAF Heimdall 2.11.6 through 2.13.x before 2.14.0, an SSRF issue allows remote attackers to access internal network resources via the Tenable proxy endpoint. This occurs in apps/backend/src/tenable/tenable.controller.ts.	2026-08-29	5.8	CVE-2026-82477
moghtech--komodo	Komodo through 2.3.2 discloses internal resource identifiers and writes audit entries before performing permission checks in the /execute and /execute/{variant} handlers. Authenticated users can guess resource names to obtain internal identifiers and insert fraudulent audit log entries misrepresenting privileged operations.	2026-08-28	5.4	CVE-2026-82267
MongoDB--BI Connector	An unauthenticated client that can reach a MongoDB Connector for BI deployment configured with Kerberos authentication may cause mongosqld to terminate when a crafted authentication exchange encounters a specific GSSAPI error-handling condition. This can interrupt BI Connector availability until the process restarts.	2026-08-27	5.9	CVE-2026-75159
MongoDB--BI Connector	In MongoDB Connector for BI, the description text of a collection's JSON schema validator is incorporated into the comment text of the DDL returned by SHOW CREATE statements without complete escaping of backslash characters. A user with permission to modify a collection's schema validator, in deployments configured to build their SQL schema from those validators, can cause additional SQL text to be embedded in that generated output. If an operator or automated tool later replays that generated statement against a SQL server, the additional text is executed with the privileges of that session.	2026-08-28	5.2	CVE-2026-77184
MongoDB--BI Connector	In MongoDB Connector for BI, mongodrdl may write a TLS private-key password to standard error when the password is supplied through both the connection URI and the corresponding command-line option. A local user with access to the captured command output and encrypted key file may use the disclosed password to access the associated TLS client key.	2026-08-27	4.4	CVE-2026-75573
MongoDB--BI Connector	The MongoDBSQL Transition Readiness Tool writes database and collection names into its generated CSV reports without neutralizing leading characters that	2026-08-28	6.3	CVE-2026-76797

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Transition Readiness Report	spreadsheet applications treat as formulas. A user with write privileges on the cluster can choose a namespace name that is later evaluated as a formula when an operator opens the generated report in a spreadsheet application, which may result in unintended disclosure of report contents or execution of external content on the operator's workstation. Generating a report for the affected namespace and opening it in a spreadsheet application is required.			
MongoDB--BI Connector Transition Readiness Report	The MongoDB Transition Readiness Tool writes query text and user names read from BI Connector log files into its generated HTML report without encoding them for that output context. A user able to issue queries through the BI Connector can influence log content so that markup supplied in a query is interpreted by the browser when an operator later generates and opens the report, which may disclose other users' logged query text and user names to an external party or present misleading content to the operator. Generating a report over logs containing the affected entries and opening that report in a browser is required.	2026-08-28	6.3	CVE-2026-76798
MongoDB--BI Connector Transition Readiness Report	MongoSQL Transition Readiness Tool does not sufficiently encode database metadata before including it in generated HTML. A MongoDB user with write access can introduce crafted metadata that may cause script code to run when another user generates and opens the report, potentially exposing report contents or altering its display.	2026-08-28	4.6	CVE-2026-76794
MongoDB--C Driver	A weakness in the MongoDB C Driver allows special elements in caller-supplied database and collection name components to pass without sanitization when the driver composes the target namespace for an operation. An application that incorporates untrusted input into these name components can have operations directed at a resource other than the one intended.	2026-08-27	5.4	CVE-2026-81524
MongoDB--C# Driver	A NoSQL/expression injection weakness exists in the LINQ-to-aggregation query translation layer of the MongoDB C# Driver, in both aggregation expression and query filter translation. When application-supplied values are embedded in certain query constructs, special elements contained within those values are not properly escaped before the resulting query is transmitted to the database, so portions of the value may be interpreted by the database as query logic rather than as data. A user able to supply values that an application incorporates into an affected query may thereby cause unintended data to be returned or query results to be altered.	2026-08-27	6.5	CVE-2026-81527
MongoDB--C# Driver	A MongoDB C# driver document-replacement code path omits the element-name/shape validation that the equivalent write paths apply, so a value supplied as a replacement is forwarded to the server without neutralization of query-language special elements. An application that passes untrusted, loosely-typed input as a replacement value therefore allows that input to be interpreted by the database as update logic rather than as data, executing under the application's own database credentials. Applications using strongly-typed document mappings are not affected.	2026-08-27	5.4	CVE-2026-81528
MongoDB--C# Driver	A weakness in the client-side encryption configuration surface of the MongoDB C# Driver causes sensitive key-management credential material supplied by the application to be reproduced verbatim in the driver's human-readable diagnostic representation of its client settings, instead of being masked as other secret fields are. A party able to read the application's logs, diagnostic output, or a process memory dump may thereby recover the plaintext credentials and use them to decrypt protected field data.	2026-08-27	5.6	CVE-2026-81530
MongoDB--GO Driver	The MongoDB Go Driver's client-level bulk write operation may accept a caller-supplied database name containing a reserved separator character without escaping it before the name is used to build the target namespace for the operation. An application that passes untrusted input as a database name could therefore have the write directed at a database and collection other than the ones it intended. Only the Client.BulkWrite API is affected.	2026-08-27	6.5	CVE-2026-81521

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MongoDB--libmongocrypt	A missing input-validation issue in MongoDB libmongocrypt's automatic-encryption context setup allows a caller-supplied database identifier to be accepted without sanitization. The resulting impact is limited to incorrect schema selection, which may lead to limited disclosure or modification of information handled by the application.	2026-08-27	4.4	CVE-2026-81523
MongoDB--Rust Driver	The MongoDB Rust Driver does not neutralize special characters in a caller-supplied target identifier before embedding it in the request it sends to the server. An actor able to influence that identifier in an application using the driver may cause write operations to be applied to an unintended target within the same deployment using the application's own credentials. This may result in unauthorized modification of data belonging to another logical boundary enforced by the application.	2026-08-27	6.5	CVE-2026-81526
morgan--morgan	morgan is an HTTP request logger middleware for Node.js. In versions prior to 1.12.0, the internal helper that escapes log token values did not neutralize the Unicode line separator characters U+0085 (Next Line), U+2028 (Line Separator), and U+2029 (Paragraph Separator). An unauthenticated remote client can place these characters in an attacker-controlled log token, for example a Basic auth username surfaced through the remote-user token, so that Unicode-aware downstream log processing splits a single request log into multiple logical records. This is a log forging issue (CWE-117) and an incomplete-fix follow-up to CVE-2026-5078, which only addressed ASCII control characters. The issue is fixed in morgan 1.12.0, which extends the escaping set to cover these Unicode line separators. Upgrade to morgan 1.12.0 to remediate.	2026-08-28	5.3	CVE-2026-15603
MuffinGroup--Betheme	The Betheme theme for WordPress is vulnerable to Stored Cross-Site Scripting via the theme's 'icon_box_2' shortcode in all versions up to, and including, 28.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-26	6.4	CVE-2026-6178
Murali--Push Notification for Post and BuddyPress	Subscriber Broken Access Control in Push Notification for Post and BuddyPress <= 3.20 versions.	2026-08-27	5.4	CVE-2026-81279
Murrelektronik--Xelity 4TX M GE	The web GUI of affected Murrelektronik Xelity switches logs MAC addresses from the devices MAC address table when an authenticated administrator uses the 'Copy learned MAC Addresses' function. Due to improper generation of error messages, an unauthenticated attacker with network access to the web interface can retrieve the logged MAC addresses via browser developer tools.	2026-08-24	5.3	CVE-2026-8173
Nagios Enterprises, LLC.--Nagios Core	Nagios Core before 4.5.12 contains a cross-site request forgery vulnerability in cmd.cgi where the CSRF protection mechanism passes validation when the NagFormId cookie is absent. Attackers can craft a malicious cross-site POST request to execute arbitrary Nagios commands as a currently authenticated user without their knowledge or consent.	2026-08-26	6.5	CVE-2026-48548
Nagios Enterprises, LLC.--Nagios Core	Nagios Core before 4.5.13 and Nagios XI before 2026R1.5 contains a CSRF vulnerability in cmd.cgi. When no Cookie header is present, the double-submit cookie protection can be bypassed by supplying matching NagFormId and nagFormId values in the POST body, allowing a cross-site request to execute Nagios commands as a currently authenticated user.	2026-08-26	6.5	CVE-2026-48549
NASA--cFS	A vulnerability was identified in NASA cFS up to 7.0.1. Impacted is the function OS_read of the file modules/protocol/tcp/fsw/src/sbn_tcp_if.c of the component SBN TCP Module. Such manipulation of the argument MsgSz leads to buffer overflow. The attack must be carried out from within the local network. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-30	6.3	CVE-2026-82479

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
netweblogic-- Events Manager Calendar, Bookings, Tickets, and more!	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 7.3.7.4 via the em_options_save function. This makes it possible for authenticated attackers, with administrator-level access and above, to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included. The stored traversal key is subsequently executed via an include_once() call that fires on every admin_init invocation - including unauthenticated admin-ajax.php requests - meaning once the malicious key is stored by an administrator, the inclusion is triggered without any further authentication or capability check.	2026-08-25	6.6	CVE-2026-14280
netweblogic-- Events Manager Calendar, Bookings, Tickets, and more!	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to generic SQL Injection via Stored 'meta_key' via Event/Location Duplicate Action in all versions up to, and including, 7.4.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. This is a second-order SQL injection: an attacker first plants SQL metacharacters in a custom meta key via the standard add-meta flow (WordPress stores these verbatim in wp_postmeta), then triggers the injection by invoking the event_duplicate or location_duplicate action, which reads the stored meta keys via get_post_meta() and concatenates them unsafely into the INSERT query.	2026-08-25	6.5	CVE-2026-15023
netweblogic-- Events Manager Calendar, Bookings, Tickets, and more!	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'header_format' parameter in all versions up to, and including, 7.4.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The shortcode entry point sanitizes 'header_format' via wp_kses(), but the unauthenticated 'search_events_grouped' AJAX action bypasses this sanitization entirely, leaving the parameter unsanitized before it is echoed into the HTML body in output_grouped().	2026-08-25	6.1	CVE-2026-17089
netweblogic-- Events Manager Calendar, Bookings, Tickets, and more!	The Events Manager - Calendar, Bookings, Tickets, and more! plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 7.4.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to view the titles, dates, descriptions, and location details of events and locations that administrators have marked as draft, pending, trashed, or private.	2026-08-25	5.3	CVE-2026-10627
nextendweb-- Smart Slider 3	The Smart Slider 3 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'slider' Block Attribute in all versions up to, and including, 3.5.1.38 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected scripts execute specifically when a user opens the affected post in the WordPress block editor, making Editors and Administrators the primary targets.	2026-08-28	6.4	CVE-2026-15798
NI--LabVIEW	There is an integer conversion vulnerability resulting in an out-of-bounds read when loading images recently discovered in NI LabVIEW. This may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user to open a specially crafted VI file. This vulnerability affects NI LabVIEW 2026 Q3 and prior versions.	2026-08-25	6.6	CVE-2026-18444
NI--LabVIEW	There is an integer overflow vulnerability resulting in an out-of-bounds write recently discovered in NI LabVIEW. This may result in information disclosure or arbitrary code execution. Successful exploitation requires an attacker to get a user	2026-08-25	6.6	CVE-2026-18445

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to open a specially crafted VI file. This vulnerability affects NI LabVIEW 2026 Q3 and prior versions.			
nltk--nltk	NLTK versions before 3.10.3 contain a path traversal vulnerability in corpus readers that reopen root-derived paths using built-in open() instead of nltk.pathsec.open(), allowing symlinks to escape trusted roots. Attackers who stage symlinked corpus files under a trusted data root can disclose outside-root content through normal corpus reader methods like channels(), domains(), and synonyms().	2026-08-25	5.9	CVE-2026-79676
nltk--nltk	NLTK before 3.10.3 contains a regular expression denial of service (ReDoS) vulnerability in the tgrep module. The _tgrep_node_action function compiles user-supplied regular expressions embedded in /regex/ pattern nodes and executes them via re.search against tree node labels without any validation or timeout. An attacker who controls the tgrep pattern (e.g., via tgrep_positions() or tgrep_compile() exposed to external input) can supply a pattern that triggers catastrophic backtracking, causing indefinite CPU saturation that blocks the Python process.	2026-08-26	5.9	CVE-2026-80206
nltk--nltk	NLTK before 3.10.3 contains an uncontrolled recursion vulnerability in nltk.featurize.FeatStructReader that allows unauthenticated attackers to cause a denial of service by supplying deeply nested feature-structure input. Attackers can craft trivial payloads with nested brackets that exceed Python's recursion limit and raise an unhandled RecursionError, crashing applications that parse user-supplied feature structures or feature grammars.	2026-08-27	5.3	CVE-2026-81724
NousResearch--hermes-agent	Hermes Agent 0.16.0 prior to 0.17.0 contains an improper path restriction vulnerability that allows attackers who can influence ingested message content to overwrite the credential store by bypassing sensitive-path guards that excluded the auth.json file. Attackers can craft malicious messages directing the agent's file-write tooling to overwrite the credential store without triggering any path-based protection, enabling credential tampering or unauthorized access.	2026-08-28	6.8	CVE-2026-82020
NVIDIA--DGX Spark	NVIDIA DGX Spark contains a vulnerability in the standalone MM firmware where an attacker could be able to cause an out-of-bounds read. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-25	6	CVE-2026-24225
NVIDIA--DGX Spark	NVIDIA DGX Spark contains a vulnerability in UEFI where a Attacker may cause a/an CWE-693 by privileged local user. A successful exploit of this vulnerability may allow an attacker to bypass administrator password protection in UEFI.	2026-08-25	6	CVE-2026-47624
NVIDIA--NemoClaw	NVIDIA NemoClaw contains a vulnerability where an attacker could cause insufficiently protected credentials . A successful exploit of this vulnerability might lead to information disclosure and data tampering.	2026-08-25	5.6	CVE-2026-65087
NVIDIA--NemoClaw	NVIDIA NemoClaw contains a vulnerability where an attacker could cause invocation of process using visible sensitive information. A successful exploit of this vulnerability might lead to information disclosure.	2026-08-25	5.5	CVE-2026-65088
NVIDIA--OpenShell	NVIDIA OpenShell for Linux contains a vulnerability in its sandbox exec handler, where an attacker could cause an OS command injection. A successful exploit of this vulnerability might lead to code execution, information disclosure, and data tampering.	2026-08-25	6.8	CVE-2026-65086
NVIDIA--OpenShell	NVIDIA OpenShell for Linux contains a vulnerability in its inference proxy, where an attacker could cause an improper encoding or escaping of output. A successful exploit of this vulnerability might lead to information disclosure and data tampering.	2026-08-25	5.2	CVE-2026-65085
NVIDIA--Unified Fabric Manager Enterprise - GA	NVIDIA UFM Enterprise contains a vulnerability in the user management component, where an authenticated administrator could inject commands by sending a crafted API request. A successful exploit of this vulnerability might lead to code execution, escalation of privileges and information disclosure.	2026-08-25	6.8	CVE-2026-24167

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NVIDIA--Unified Fabric Manager Enterprise - GA	NVIDIA UFM Enterprise contains a vulnerability in the IBDiagnet API where an authenticated attacker with administrative privileges may cause command injection by sending crafted API requests. A successful exploit of this vulnerability may lead to code execution, escalation of privileges and information disclosure.	2026-08-25	6.8	CVE-2026-24168
NVIDIA--Unified Fabric Manager Enterprise - GA	NVIDIA UFM Enterprise contains a vulnerability in the session management component, where an attacker could use a hard-coded cryptographic key to extract information. A successful exploit of this vulnerability might lead to information disclosure and escalation of privileges.	2026-08-25	5.1	CVE-2026-24166
Okta--Okta Privileged Access Client	The Okta Privileged Access client does not reject a leading hyphen in the username portion of an SSH target. As a result, the value may be interpreted as a command-line option by the underlying SSH process.	2026-08-25	5.3	CVE-2026-77585
Open Asset Import Library--Assimp	A security vulnerability has been detected in Open Asset Import Library Assimp up to 6.0.2. The impacted element is the function MD5Importer::MakeDataUnique of the file code/AssetLib/MD5/MD5Loader.cpp. The manipulation of the argument iNewIndex leads to heap-based buffer overflow. The attack can only be performed from a local environment. The identifier of the patch is bf9dabb617c46e5133dac65cca6bff177917afcb. Applying a patch is the recommended action to fix this issue.	2026-08-30	5.3	CVE-2026-82591
Open-Xchange GmbH--OX Dovecot CE	An unauthenticated attacker can send a truncated quoted argument to the ManageSieve login process, which makes it spin in an infinite loop consuming CPU. This can cause degradation or denial of service for Sieve script management, and repeated connections can consume all available CPU on the server. Monitor system for abnormal CPU usage and kill the offending process. Restrict network access to the ManageSieve service to trusted clients. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	5.9	CVE-2026-40019
Open-Xchange GmbH--OX Dovecot Pro	An attacker that can send mail to a user can craft a message header that makes the IMAP THREAD command consume CPU disproportionate to the size of the message. When a mail client issues a THREAD command on the affected mailbox, this can cause degradation or denial of service for IMAP. Monitor system for abnormal CPU usage, kill the offending process and remove the offending message from the affected mailbox. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	6.5	CVE-2026-40014
Open-Xchange GmbH--OX Dovecot Pro	An attacker that can send mail to a user can craft a message header whose values are chosen to collide in an internal hash table, which makes the IMAP THREAD command consume CPU disproportionate to the size of the message. This is a separate issue from CVE-2026-40014 and is not addressed by that fix. Whenever a mail client issues a THREAD command on the affected mailbox, this can cause degradation or denial of service for IMAP. Monitor system for abnormal CPU usage, kill the offending process and remove the offending message from the affected mailbox. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	6.5	CVE-2026-40017
Open-Xchange GmbH--OX Dovecot Pro	An attacker that has valid credentials can select a compression algorithm for the IMAP connection whose decompression state requires a large amount of memory, and open several such connections. The memory limit of the process is reached with only a few connections, terminating the process and all connections it handles, which can cause degradation or denial of service for IMAP. Disable IMAP compression. Alternatively limit the number of connections handled by a single imap-login process, though this has a performance impact. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	6.5	CVE-2026-52687
Open-Xchange GmbH--OX Dovecot Pro	An attacker that has valid credentials can send crafted compressed data that causes the affected process to exhaust its stack and crash. The affected process is terminated, which can cause degradation or denial of service for IMAP. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	6.5	CVE-2026-73209

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Open-Xchange GmbH--OX Dovecot Pro	An attacker that can get Dovecot to relay a message, for example through Sieve redirect or submission relay, can use a crafted line ending in the message body to bypass the outbound protection that prevents message content from being interpreted as SMTP commands. A downstream mail server that hasn't yet fixed the SMTP smuggling vulnerability can be tricked into treating part of the message body as new SMTP commands, allowing injection of spoofed email. This is the same vulnerability class as CVE-2023-51764 and CVE-2023-51766. Where you control the receiving mail servers, ensure they reject bare carriage returns in message data. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	5.9	CVE-2026-33604
Open-Xchange GmbH--OX Dovecot Pro	An attacker that holds an OAuth2 token granting only part of the required scopes can authenticate, because when more than one scope is required in the configuration, the remote token validation paths accept a token that carries only one of them, while the local token validation path correctly requires all of them. The configured authorization policy is not enforced, so a token that was granted only part of the required permissions is accepted where it should have been rejected. Use local token validation where tokens can be validated locally. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	5.9	CVE-2026-40205
Open-Xchange GmbH--OX Dovecot Pro	When mail_max_userip_connections is set (default 10) and reached, submission-login can crash with epoll() panic caused by file descriptor handling issues. If running in high-security mode (default for community releases), only the new submission connection gets terminated. If running in high-performance mode (default for Pro releases), all connections handled by the submission-login process will be terminated. The crashes can cause failure for user to send a message, or it can cause duplicate messages to be sent. If TLS is not used (in the backend server processing the submission), duplicate deliveries cannot happen, because the crash can only happen at AUTH stage. Limit the number of connections handled by single submission-login process. This has a performance impact though. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	4.3	CVE-2026-33263
Open-Xchange GmbH--OX Dovecot Pro	Mail content stored by a user can be crafted so that it is interpreted as dsync protocol commands when an administrator later runs dsync with the stream protocol, for example during a migration. Injected commands can modify mailbox state on the destination during migration or replication, including internal mailbox attributes that a user should not be able to set directly. It can also cause dsync errors. Avoid running dsync with the stream protocol on mailboxes with untrusted content. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	4.8	CVE-2026-33606
Open-Xchange GmbH--OX Dovecot Pro	An attacker that has valid credentials can use IMAP LIST command to consume CPU. This can cause degradation or denial of service for IMAP. Monitor system for abnormal CPU usage and kill the offending process and lock account. Alternatively install fixed version. No publicly available exploits are known.	2026-08-28	4.3	CVE-2026-33607
Open-Xchange GmbH--OX Dovecot Pro	An attacker that has valid credentials can submit a Sieve script containing an extreme numeric literal, which causes an out-of-bounds write when the ManageSieve service compiles the script. This causes memory corruption and an observed crash of the ManageSieve process, resulting in denial of service for script management. This might be able to be used for remote code execution. Disable the ManageSieve service if users do not need remote Sieve script management. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	4.3	CVE-2026-40013
Open-Xchange GmbH--OX Dovecot Pro	An attacker that has valid credentials can open many connections to the imap-hibernate service and send invalid commands, which can intermittently cause an out-of-bounds read and crash the process. The crash interrupts hibernated IMAP sessions handled by the affected process, which can cause degradation of service for IMAP. Disable IMAP hibernation. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	4.3	CVE-2026-40015

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Open-Xchange GmbH--OX Dovecot Pro	Forwarding information received from a host listed as a trusted proxy is not kept separate from Dovecot's own authentication fields, so a value sent by that host can be injected as an internal authentication field. Any host permitted to act as a trusted proxy can authenticate as any user without knowing that user's password. This affects deployments whose password database honours a field that permits authentication without a password. Deployments that do not configure trusted proxies are not affected. Restrict the list of trusted proxy networks to hosts that are fully under your control. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	4.3	CVE-2026-42008
Open-Xchange GmbH--OX Dovecot Pro	An attacker that has valid credentials can send an invalid IMAP URLFETCH command, which causes uninitialized memory to be included in the error response returned to the client. Process memory contents can be disclosed to the client, which may include sensitive data. Disable the IMAP URLAUTH functionality. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	4.3	CVE-2026-42392
Open-Xchange GmbH--OX Dovecot Pro	A host listed as a trusted proxy can send forwarding information containing a NUL byte, which crashes the login process on the following login attempt. The login process is terminated, which can cause degradation or denial of service for logins. Deployments that do not configure trusted proxies are not affected. Restrict the list of trusted proxy networks to hosts that are fully under your control. Update to non-vulnerable version. No publicly available exploits are known.	2026-08-28	4.3	CVE-2026-42395
Open5GS--Open5GS	A flaw has been found in Open5GS 2.8.0. This vulnerability affects unknown code of the component AMF UEContextReleaseRequest Path Handler. Executing a manipulation can lead to improper authorization. It is possible to launch the attack remotely.	2026-08-24	6.3	CVE-2026-78158
Open5GS--Open5GS	A flaw has been found in Open5GS up to 2.8.0. This affects an unknown function of the file src/hss/hss-cx-path.c of the component HSS. This manipulation of the argument User-Name causes reachable assertion. The attack is possible to be carried out remotely. The exploit has been published and may be used. Patch name: c9abe09421eb99bbf1cd7862a3d375e58a4eb9e4. It is recommended to apply a patch to fix this issue.	2026-08-24	4.3	CVE-2026-78186
Open5GS--Open5GS	A vulnerability was determined in Open5GS up to 2.7.7. This vulnerability affects the function amf_namf_comm_decode_ue_mm_context_list of the file src/amf/namf-handler.c of the component AMF. This manipulation of the argument ueContext.mmContextList[*].allowedNssai causes memory corruption. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.8.0 is able to resolve this issue. Patch name: abf8a836564b966b5141110fc25ed413c4f17522. It is recommended to upgrade the affected component.	2026-08-30	4.3	CVE-2026-82587
Open5GS--Open5GS	A vulnerability was identified in Open5GS up to 2.7.7. This issue affects some unknown processing of the file src/amf/namf-handler.c of the component Transfer Endpoint. Such manipulation leads to null pointer dereference. The attack can be launched remotely. Upgrading to version 2.8.0 is capable of addressing this issue. The name of the patch is abf8a836564b966b5141110fc25ed413c4f17522. Upgrading the affected component is advised.	2026-08-30	4.3	CVE-2026-82588
Open5GS--Open5GS	A security flaw has been discovered in Open5GS up to 2.7.7. Impacted is the function amf_namf_comm_handle_n1_n2_message_transfer of the file src/amf/namf-handler.c of the component N1-N2 Message Handler. Performing a manipulation of the argument N1N2MessageTransferReqData.n2InfoContainer.smInfo.n2InfoContent.ngapleType results in denial of service. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 2.8.0 is recommended to address this issue. The patch is named abf8a836564b966b5141110fc25ed413c4f17522. It is advisable to upgrade the affected component.	2026-08-30	4.3	CVE-2026-82589

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Open5GS-- Open5GS	A weakness has been identified in Open5GS up to 2.7.7. The affected element is the function <code>smf_nudm_sdm_handle_get</code> of the file <code>src/smf/nudm-handler.c</code> of the component SMF. Executing a manipulation of the argument <code>preemptCap</code> can lead to reachable assertion. The attack may be launched remotely. Upgrading to version 2.8.0 is sufficient to fix this issue. This patch is called 4554405f29bffd7562abedbee63484825bd90cd5. You should upgrade the affected component.	2026-08-30	4.3	CVE-2026-82590
openfaas--faas	The OpenFaaS gateway registers <code>GET /system/telemetry</code> in <code>gateway/main.go</code> and, when <code>basic_auth</code> is enabled, wraps each administrative <code>/system/*</code> handler in <code>auth.DecorateWithBasicAuth</code> . <code>TelemetryHandler</code> was left out of that wrap block from 0.27.11, which introduced the route, until 0.27.14, which added it. On an affected gateway the route therefore reaches the forwarding proxy with no credential check and returns whatever the configured provider serves for <code>/system/telemetry</code> , so any client that can reach the gateway port can read the provider's telemetry regardless of the <code>basic_auth</code> setting. The exposed content depends on the provider, and covers resource and invocation metrics for faasd and pod or cluster state for faas-netes.	2026-08-27	5.3	CVE-2026-81664
openNDS-- openNDS	Multiple memory leaks in openNDS before 11.0.0 allow an unauthenticated attacker on the captive portal network to exhaust all available memory on the device within minutes.	2026-08-28	5.3	CVE-2026-38819
openzipkin--zipkin	Zipkin through 3.6.1 exposes Spring Boot Actuator endpoints on the tracing API port without authentication, allowing unauthenticated attackers to access sensitive information. Attackers can read environment variables, bean configurations, and storage credentials via actuator endpoints, or modify log levels to suppress logging.	2026-08-28	6.5	CVE-2026-82265
Oracle Corporation-- Oracle Java SE	Vulnerability in Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u511. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	2026-08-26	6.5	CVE-2026-71054
oras-project--oras	ORAS (OCI Registry As Storage) is a CLI and library for managing artifacts in OCI registries. In ORAS CLI versions up to and including 1.3.2, the recursive referrer traversal does not track visited descriptors, so a malicious OCI registry that returns a cyclic referrer graph causes unbounded recursion and memory growth. This affects oras discover, whose recursive traversal is enabled by default because the <code>--depth</code> option defaults to 0 (unlimited), as well as the recursive referrer counting used by the oras backup and oras restore workflows. A cyclic graph can be as simple as A referring to B and B referring back to A. A malicious registry can use this to cause a client-side denial of service, exhausting CPU and memory and hanging automation or CI/CD pipelines that run ORAS against untrusted registry metadata. The vulnerability does not extend to code execution, artifact substitution, or integrity bypass. This issue has been fixed in version 1.3.3.	2026-08-25	6.5	CVE-2026-55588
pac4j--pac4j	<code>pac4j-oidc</code> before 6.5.6 accepts OIDC callbacks carrying only an access token without authorization code or ID token validation. Attackers can substitute access tokens minted for other clients to create authenticated sessions without proper issuer, audience, nonce, or subject verification.	2026-08-29	6.5	CVE-2026-82462
pac4j--pac4j	<code>pac4j-core</code> before 6.5.6 contains an open redirect vulnerability in <code>DefaultLogoutLogic.perform()</code> that accepts backslash-prefixed logout redirect	2026-08-29	6.1	CVE-2026-82464

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	targets matching logoutUrlPattern. Attackers can craft logout links with backslash-prefixed external hosts that browsers normalize into network-path references, redirecting victims to attacker-controlled sites after logout.			
pac4j--pac4j	pac4j-saml before 6.5.6 does not require signature validation of SAML LogoutRequest messages in SAML2LogoutValidator.validateLogoutRequest(). When an IdP sends no SessionIndex, a session can be destroyed based solely on the NameID, allowing an unauthenticated attacker to submit an unsigned LogoutRequest with a guessed identifier (e.g., an email address used as NameID) to terminate a victim's SAML session.	2026-08-29	5.3	CVE-2026-82465
perber--leafwiki	LeafWiki extracts an uploaded ZIP archive without limiting how much data it will write. ZipExtractor.ExtractToDir in internal/importer/zip_extractor.go opens each entry and copies it to the destination with io.Copy, which runs to the end of the decompressed stream, so only the size of the uploaded archive is bounded and the size it expands to is not. The import route that reaches this code requires the Editor or Admin role, and the upload itself is capped at 500 MiB compressed. Because a ZIP entry can compress at a very high ratio, an archive well inside that cap can expand to hundreds of gigabytes as it is written out. The extraction directory defaults to a location under the operating system temporary directory, so the written data consumes the disk backing that path, which on a tmpfs-backed temporary directory is memory. A user holding the Editor role can therefore exhaust the storage the service depends on and keep it from serving, using far more resource than the upload limit alone would permit.	2026-08-25	6.5	CVE-2026-80189
peterschulznl--WP Data Access App Builder for Tables, Forms, Charts, Maps & Dashboards	The WP Data Access plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.5.68 via the 'check_app_access' function due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to access data from protected app containers by exploiting a mismatch between the authorization check (performed against app_id) and data retrieval (performed using cnt_id without verifying container ownership).	2026-08-26	5.3	CVE-2026-3235
PHPGurukul--Student Information System	A weakness has been identified in PHPGurukul Student Information System 1.0. Affected by this vulnerability is an unknown functionality of the file /student_edit1.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	2026-08-29	6.3	CVE-2026-82424
PLANET Technology Corp.--PLANET GS-4210-16P2S	PLANET GS-4210-16P2S firmware before 3.441b260626 contains an authenticated null pointer dereference vulnerability in /cgi-bin/dispatcher.cgi. The web_poe_alive_rmtip_post handler dereferences the rmtIP parameter without verifying its presence. A remote authenticated attacker can send a crafted request omitting the rmtIP parameter to cause the CGI process to dereference a null pointer and crash, resulting in denial of service of the web management interface.	2026-08-28	4.9	CVE-2026-75125
PLANET Technology Corp.--PLANET GS-4210-16P2S	PLANET GS-4210-16P2S firmware before 3.441b260626 contains multiple authenticated stack buffer overflow vulnerabilities in /cgi-bin/dispatcher.cgi. The following handlers copy attacker-controlled POST parameters into fixed-size stack buffers without length validation: web_vlan_membership_edit_dialog_post; web_dai_vlan_post; web_poe_alive_rmtip_post; web_sys_snmp_post; web_tool_upgradeManager_post; web_port_countersClr_post; web_rmon_statisticsClr_post; web_cablediag_copper_post; web_aaa_*Authlist* handlers; web_acl_mgmt_Rules_Apply_post; web_acl_mgmt_Rules_Edit_post; web_acl_*AceDel_post handlers; web_acl_*AceAdd/Edit_post handlers; web_acl_bindAdd_post; web_acl_bindEdit_post; web_snmp_v3view_add_post; web_snmp_v3group_add_post; web_snmp_v3community_add_post; web_snmp_v3host_add_post; web_snmp_notifyv3_add_post; web_snmp_v3user_add_post; web_snmpv3_remote_engineld_add_post; web_stp_globalSetting_post; web_isg_db_post; web_tacplus*_post handlers; web_dhcp_option82_post; and web_dhcp_port_option82_cid_post. A remote	2026-08-28	4.9	CVE-2026-75126

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attacker can send crafted requests to crash the CGI process or web management service, resulting in denial of service.			
PLANET Technology Corp.-- PLANET GS-4210-16P2S	PLANET GS-4210-16P2S firmware before 3.441b260626 contains authenticated stack buffer overflow and null pointer dereference vulnerabilities in /cgi-bin/dispatcher.cgi. The web_radiusSrv*_post family of handlers copies the radKey, radKey_0, radDftParamKey, radName, and radlp POST parameters into fixed-size stack buffers without length validation, and additionally dereferences radName and radlp without verifying their presence in the request. A remote authenticated attacker can send crafted requests to crash the CGI process or web management service, resulting in denial of service.	2026-08-28	4.9	CVE-2026-77217
PLANET Technology Corp.-- PLANET GS-4210-16P2S	PLANET GS-4210-16P2S firmware before 3.441b260626 contains authenticated stack buffer overflow vulnerabilities in /cgi-bin/dispatcher.cgi. The web_login_first_post handler copies the usrPass POST parameter into a fixed-size stack buffer without length validation, the web_sys_enablePasswd_post handler copies the enbPass POST parameter into a fixed-size stack buffer without length validation, and the web_sys_localUser_post handler copies the usrName and usrPass POST parameters into fixed-size stack buffers without length validation. A remote authenticated attacker can send a crafted request to crash the CGI process or web management service, resulting in denial of service.	2026-08-28	4.9	CVE-2026-77218
pocket-id--pocket-id	Pocket ID is an OIDC provider that allows users to authenticate with their passkeys to services. From 2.6.0 until 2.9.0, frontend/src/routes/authorize/+page.ts reads the redirect_uri query parameter and frontend/src/routes/authorize/+page.svelte uses the raw callbackURL in redirectWithError when prompt=none cannot complete silent authorization. The client-side path only blocks javascript and data schemes and does not invoke the backend callback allow-list validation, so an unauthenticated attacker who knows a valid client_id can redirect a victim browser to an arbitrary HTTP or HTTPS origin for phishing or OIDC error and state smuggling. This issue is fixed in version 2.9.0.	2026-08-28	4.3	CVE-2026-55834
pollen-robotics-- rechy_mini	Rechy Mini is an SDK for controlling Rechy Mini robots. Prior to 1.8.2, the Rechy Mini daemon exposes the /api/media/sounds/upload endpoint implemented by the upload_sound method in src/rechy_mini/daemon/app/routers/media.py without authentication, file-extension checks, content validation, or size validation. The daemon binds to 0.0.0.0 by default and uses permissive CORS allow_origins=["*"], allowing an unauthenticated network attacker to upload arbitrary file types that are written to /tmp/rechy_mini_sounds/<original_filename>. Malicious files can compromise stored-data integrity and can serve as a foothold when combined with other vulnerabilities. This issue is fixed in version 1.8.2.	2026-08-25	5.3	CVE-2026-55419
PrivateBin-- PrivateBin	PrivateBin is an online pastebin where the server has zero knowledge of pasted data. Prior to 2.0.5, AttachmentViewer.setAttachment in js/privatebin.js uses getAttachmentMimeType to accept attacker-controlled MIME types and uses getBlobUrl to create a same-origin blob before setting attachmentLink's href for the Download attachment link. The SVG-only sanitization branch updates only the preview blob, so text/html, image/svg, application/xhtml+xml, and text/xml attachments can remain active in the download blob. On an instance with fileupload = true and a weakened, stripped, or absent Content Security Policy, an anonymous attacker can create such an attachment, and a victim who opens the link in a new tab causes inline JavaScript to execute in the PrivateBin origin. The script can read origin-scoped local storage and issue same-origin requests, including requests to applications co-hosted on the same domain. This issue is fixed in version 2.0.5.	2026-08-28	4.3	CVE-2026-55696
provectus--kafka-ui	A security flaw has been discovered in provectus kafka-ui up to 0.7.2. The affected element is the function executeSmartFilterTest of the file kafka-ui-api/src/main/java/com/provectus/kafka/ui/controller/MessagesController.java of the component Groovy Code Handler. The manipulation results in code injection.	2026-08-24	6.3	CVE-2026-78166

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The attack may be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.			
rcclone--rcclone	rcclone versions >= v1.72.0 and <= v1.74.4 (fixed in v1.75.0) contain multiple denial-of-service vulnerabilities in the archive backend's SquashFS parser, which relies on the github.com/diskfs/go-diskfs dependency. The parser fails to validate attacker-controlled superblock and metadata values before use. An attacker who can place or modify a SquashFS image in storage exposed through an rclone :archive: remote can craft a malicious image that triggers an integer division-by-zero panic (zero block size), an out-of-bounds slice panic (out-of-range inode metadata offset), or a non-progress CPU loop (truncated metadata stream). Variants 1 and 2 terminate the rclone process and, via 'rclone serve sftp', can crash the entire SFTP server; variant 3 causes sustained CPU consumption. Parsing is lazy, so a victim or remote client must address or descend into the malicious archive object to trigger it.	2026-08-25	6.5	CVE-2026-79775
rcclone--rcclone	rcclone serve s3 before 1.74.4 contains a path traversal vulnerability that allows attackers to read and overwrite root-level files by using dot-dot segments in S3 object keys. Attackers can send requests with object keys like ../root-secret.txt to escape the bucket namespace and access files in the serve root directory.	2026-08-25	6.5	CVE-2026-79781
rcclone--rcclone	rcclone before 1.75.0 mounts the pprof debug handler as its own router route, bypassing the fail-closed authentication rule in the main handler. Attackers can access the /debug/pprof/cmdline endpoint unauthenticated to retrieve the full process argv including backend credentials.	2026-08-25	5.3	CVE-2026-79776
rcclone--rcclone	rcclone before v1.75.0 contains a denial of service vulnerability in the WebDAV TUS creation handler that dereferences a nil response before checking for transport errors. A malicious or compromised configured endpoint can reset connections during TUS uploads to trigger a panic that terminates unrecovered goroutines and halts unrelated work in long-lived processes.	2026-08-25	5.3	CVE-2026-79778
rcclone--rcclone	rcclone versions before v1.75.0 fail to reject transport downgrades in redirect handling, allowing Basic authorization and Cookie headers to be replayed over plaintext HTTP after same-host HTTPS-to-HTTP redirects. An on-path attacker observing the plaintext hop can capture and reuse credentials to perform WebDAV operations with the compromised account's permissions.	2026-08-25	5.3	CVE-2026-79779
rcclone--rcclone	rcclone before v1.75.0 fails to sanitize IBM IAM bearer tokens and SSE-C encryption keys during S3 redirect callbacks, allowing credentials to be preserved across scheme or host changes. Attackers observing network traffic from a trusted endpoint can capture reusable IBM IAM tokens on same-host HTTPS-to-HTTP downgrades or SSE-C keys on cross-origin redirects to access protected S3 objects.	2026-08-25	5.3	CVE-2026-79780
rconfig--rconfig	rConfig Core 8.0.0 before 8.2.13 contains a path traversal vulnerability that allows authenticated users to read arbitrary files by supplying crafted filenames containing directory traversal sequences to the export download endpoint. Attackers can manipulate the filename parameter with traversal sequences to escape the intended export directory and access files outside it that are readable by the application process.	2026-08-24	6.5	CVE-2026-77914
Red Hat--Red Hat Ansible Automation Platform 2	A server-side request forgery (SSRF) vulnerability was found in galaxy_ng, the Ansible Galaxy server plugin for Pulp. An authenticated user with namespace management permissions can set a namespace avatar URL to an arbitrary address, including internal networks, loopback, or cloud instance metadata endpoints. A background worker fetches that URL without checking the destination, which lets the attacker probe internal services and enumerate reachable IP addresses. The HTTP client is also configured without an overall timeout, so a slow or non-responsive target can pin workers and cause a denial of service.	2026-08-25	6.4	CVE-2026-79717
Red Hat--Red Hat Ansible	A flaw was found in jwcrypto. A remote attacker can send a specially crafted JSON Web Encryption (JWE) token containing numerous period delimiters. This	2026-08-27	5.9	CVE-2026-80179

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Automation Platform 2	malformed token can force the JWE.deserialize() function to allocate excessive memory, leading to a MemoryError. This issue results in a denial of service (DoS) for services that process untrusted JWE values.			
Red Hat--Red Hat Build of Keycloak	A flaw was found in the JWT Bearer authorization grant implementation within the keycloak-services component of Red Hat Build of Keycloak. This component handles various OAuth2 and OpenID Connect grant types used for issuing access tokens. The issue occurs because the JWT Bearer grant fails to check if a client requires user consent before issuing a token. This allows an authenticated attacker with valid client credentials and a trusted identity provider assertion to bypass the consent requirement and obtain unauthorized access to a user account at a consent-gated client.	2026-08-25	5.9	CVE-2026-79652
Red Hat--Red Hat Ceph Storage 5	A flaw was found in the ipa_getkeytab module of the community.general Ansible collection. The module's bind_pw parameter, used to supply the LDAP simple-bind password when retrieving a Kerberos keytab, is not declared with no_log, unlike the sibling password parameter in the same module. As a consequence, the supplied IPA/LDAP bind password is recorded in cleartext in the managed host's system journal/syslog (the module's "Invoked with" record), is included in the module's return values and verbose (-v) output, and is displayed in Automation Controller / AWX job output. The password is additionally passed on the command line to the ipa-getkeytab helper (as --bindpw <value>), exposing it in the process list to local users while the command runs. An attacker able to read these logs, job output, or the process table can obtain the directory bind credential, potentially compromising the accounts and objects that credential can access.	2026-08-26	5.5	CVE-2026-80158
Red Hat--Red Hat Certificate System 10	A flaw was found in JSS (Java Security Services). The JSSTrustManager class does not verify NSS trust flags when validating CA certificates, allowing certificates present in the NSS database without TRUSTED_CA flags to be accepted as trust anchors for TLS connections. In non-default configurations where certificate revocation checking is disabled, this could allow a man-in-the-middle attacker to forge certificates accepted by PKI client connections.	2026-08-24	6.5	CVE-2026-78323
Red Hat--Red Hat Directory Server 11	A flaw was found in 389-ds-base. A remote, authenticated attacker could exploit a vulnerability in the Simple Authentication and Security Layer (SASL) UNBIND process. By sending a specially crafted request, the attacker can cause a connection to stall, leading to resource exhaustion and a Denial of Service (DoS) for the server.	2026-08-25	6.5	CVE-2026-78701
Red Hat--Red Hat Enterprise Linux 10	An algorithmic complexity flaw exists in libsoup's HTTP Range header processing that persists after the CVE-2025-32907 fix. CVE-2025-32907 addressed memory amplification when a client repeated the same range many times in a single Range header. Commit 9bb92f7a corrected merge correctness in soup_message_headers_get_ranges_internal() in libsoup/soup-message-headers.c, but the coalescing loop still removes merged ranges using g_array_remove_index() for each coalesced element. Because GArray is contiguous, each mid-array removal performs an O(N) memmove. When many identical satisfiable ranges are supplied (for example bytes=0-0 repeated thousands of times), the loop performs O(N^2) work coalescing them into a single range. The vulnerable path is reachable server-side from handle_partial_get() in libsoup/server/http1/soup-server-message-io-http1.c when a SoupServer handler returns HTTP 200 with a non-empty body. No authentication is required. The number of ranges is bounded only by the maximum request header size (~100 KiB), allowing roughly 25,000 ranges per request. Reporter measurements on libsoup HEAD containing the CVE-2025-32907 fix show ~90 ms single-core CPU per such request at the wire maximum, blocking the server's event loop for that duration. This is a CPU exhaustion / availability issue only. No memory corruption or information disclosure occurs. Affected: libsoup versions containing the CVE-2025-32907 fix but not merge request !550. Fixed upstream: MR !550 merged 2026-08-20, replacing per-element removal with O(N) in-place compaction and rejecting Range headers requesting more than 200	2026-08-25	5.3	CVE-2026-77680

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ranges. Upstream report: https://gitlab.gnome.org/GNOME/libsoup/-/issues/538 Related: CVE-2025-32907			
Red Hat--Red Hat Enterprise Linux 10	BlueZ sdp-xml.c type confusion via RegisterProfile(ServiceRecord) can crash bluetoothd (local DoS): a crafted nested ServiceRecord can corrupt the SDP XML parser stack so scalar union data is treated as a sequence pointer, allowing a local caller to crash bluetoothd.	2026-08-25	5.7	CVE-2026-80185
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in libsolv, a dependency-resolution library used by RPM-based package managers such as dnf and zypper to work with .solv repository cache files. When libsolv rewrites a .solv cache file, it reads directory-id values from the file's compressed filelist data without validating that they fall within the expected range. A corrupted or specially crafted .solv cache file (for example, one left in a torn state after an unclean system shutdown) can cause an out-of-bounds memory write when a tool such as dnf, yum, or zypper next processes it. Successful exploitation is expected to result in a crash of the affected tool (denial of service); it is not expected to allow arbitrary code execution because the out-of-bounds write always stores a fixed, non-attacker-controlled value.	2026-08-28	5.5	CVE-2026-82327
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in gdk-pixbuf. When loading a specially crafted JPEG image containing chunked ICC profile markers, an error during ICC profile parsing can leave stale size metadata after the profile buffer is freed. A subsequent allocation in the same decode can cause an out-of-bounds write, potentially crashing the application. To exploit this flaw, an application using gdk-pixbuf must process the malicious JPEG image. Affected version >= 2.26.4	2026-08-27	4.7	CVE-2026-81893
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in file-roller. When opening or extracting a malicious 7z or RAR archive containing a file entry with an excessively long path, file-roller's progress-line parsing copies the path into a fixed-size stack buffer using an unbounded string copy. This can trigger a stack buffer overflow and cause file-roller to terminate, resulting in a denial of service. To exploit this flaw, a victim must open or extract the crafted archive using file-roller.	2026-08-25	6.5	CVE-2026-78322
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in the file-iff (IFF/ILBM) plugin in GIMP. When processing a specially crafted IFF/ILBM image file, the plugin does not properly validate the HAM row size and improperly handles cases where the number of color planes (nPlanes) is zero. This causes a row size mismatch that bypasses memory bounds checking, resulting in heap out-of-bounds reads. This issue can result in an application crash, leading to a denial of service or a limited information disclosure of heap memory contents.	2026-08-28	6.1	CVE-2026-82324
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in the file-ico plugin in GIMP. When processing a specially crafted ICO image file, the plugin does not properly validate the used_clr (palette count) parameter. This incorrect validation leads to improper memory bounds checking, resulting in a heap out-of-bounds read. This issue can result in an application crash, leading to a denial of service or a limited information disclosure of heap memory contents.	2026-08-28	6.1	CVE-2026-82328
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in the file-pvr plugin in GIMP. When processing a specially crafted PVR image file, the VQ (compressed) decoder does not properly perform memory bounds checking. This missing validation results in a heap out-of-bounds read. This issue can result in an application crash, leading to a denial of service or a limited information disclosure of heap memory contents.	2026-08-28	6.1	CVE-2026-82330
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in the file-psd plugin in GIMP. When processing a specially crafted PSD image file, the plugin does not properly validate the channel-count parameter. This incorrect validation leads to improper memory bounds checking, resulting in both a heap out-of-bounds read and a stack out-of-bounds access. This issue can result in an application crash, leading to a denial of service or a limited information disclosure of memory contents.	2026-08-28	6.1	CVE-2026-82343

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux AI (RHEL AI) 3	A flaw was found in FFmpeg. The <code>tdsc_load_cursor()</code> function writes beyond the bounds of a heap-allocated buffer when processing crafted TDSC cursor data. A remote attacker could exploit this by supplying a specially crafted video file, potentially leading to a denial of service or arbitrary code execution.	2026-08-28	5.4	CVE-2026-18393
Red Hat--Red Hat Satellite 6	A flaw was found in Foreman. The template revision endpoint does not enforce object-level authorization when retrieving an audited template revision. An authenticated, low privileged user with a template-related permission, such as <code>view_ptables</code> , can obtain historical template contents belonging to another organization or location by supplying the corresponding audit ID. This can result in unauthorized disclosure of historical template contents, which may contain sensitive configuration information, credentials, or other secrets. The REST API revision endpoints correctly restrict this lookup.	2026-08-27	6.5	CVE-2026-81658
Red Hat--Red Hat Satellite 6	A flaw was found in Katello where the Content View Filter Rules API does not properly enforce authorization on the parent Content View Filter. An authenticated, low-privileged user with Content View permissions in one organization may be able to access and modify filter rules belonging to a Content View Filter in another organization by supplying that filter's identifier. This can result in unauthorized disclosure of filter-rule information and unauthorized changes to unpublished Content View filter configuration.	2026-08-27	5.4	CVE-2026-81668
Red Hat--Red Hat Satellite 6	A flaw was found in Katello where the Content View History API does not properly enforce authorization when accessing a Content View specified by the user. An authenticated user with permission to view Content Views in one organization may be able to access the lifecycle history of a Content View belonging to another organization by supplying its identifier to the affected API endpoint. This can result in unauthorized disclosure of Content View lifecycle information, including publication and promotion events, associated users, and timestamps.	2026-08-26	4.3	CVE-2026-79654
rexrainbow--phaser3-rex-notes	A vulnerability was identified in <code>rexrainbow phaser3-rex-notes</code> up to 1.80.17. This vulnerability affects the function <code>SetValue</code> of the file <code>plugins/utills/object/SetValue.js</code> of the component BehaviorTree Blackboard Data Interface. Such manipulation of the argument key leads to improperly controlled modification of object prototype attributes. The attack can be launched remotely.	2026-08-24	6.3	CVE-2026-78179
RocketChat--Rocket.Chat	Rocket.Chat exposes the <code>sendForgotPasswordEmail</code> Meteor method without a DDP rate limit, so an unauthenticated caller may invoke it as often as it likes. The method is reachable over DDP and over the HTTP route <code>POST /api/v1/method.callAnon/sendForgotPasswordEmail</code> , and it triggers a password reset message for any address that matches an account. With no <code>DDPRateLimiter</code> rule registered for it, a caller can drive an unbounded volume of reset mail at a chosen address from the deployment's own mail sender, and can probe addresses at scale: the method answers true for an address with no account and for a successful send, but false when the address belongs to an account that authenticates through an external provider and <code>Accounts_AllowPasswordChangeForOAuthUsers</code> is off, so repeated calls distinguish that class of account. Later versions register a rule permitting ten calls per minute per client address.	2026-08-25	5.3	CVE-2026-75575
rocq-prover--rocq	Print Assumptions does not report that a definition was produced while universe checking was disabled when that definition reaches the caller through Parameter Inline in a module type. Applying a functor inlines the body of the parameter, and the inlining drops the record that the term was built under Unset Universe Checking, so the resulting constant carries no trace of the unsafe operation. A module implementation can therefore prove False using a universe inconsistency, expose it through an inlined parameter, and have Print Assumptions report the dependent proof as closed under the global context. Because Print Assumptions is the in-process audit used to confirm that a development rests on no unexpected assumptions, a dependency built this way passes that audit while proving arbitrary propositions. The standalone checker <code>coqchk</code> does reject the resulting compiled	2026-08-24	6.3	CVE-2020-37268

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	file. The project records this in dev/doc/critical-bugs.md under non-fixed bugs and rates the risk as moderate when coqchk is not used.			
rocq-prover--rocq	The guard checker in Rocq Prover treats a parameter of a nested mutual fixpoint as uniform without examining calls between the different bodies of that fixpoint. find_uniform_parameters in kernel/inductive.ml inspects only self-recursive calls, so when no body calls itself the function concludes that every parameter is uniform. A parameter that grows through a cross-call from one body to another therefore keeps the subterm specification it inherited from the enclosing fixpoint, and a recursive call guarded by that specification is accepted although the argument is not structurally smaller. A non-terminating definition is admitted as structurally decreasing, which yields a term whose value equals its own successor and so a proof of False, from which any proposition follows. The proof requires no axioms, plugins or unsafe flags and Print Assumptions reports it as closed under the global context. Introduced in Coq 8.20 and fixed in Rocq 9.2.0.	2026-08-24	6.3	CVE-2026-72703
rocq-prover--rocq	The guard checker in Rocq Prover does not recheck the recursive tree representation of an inductive type parameter after that parameter has been changed by transport. A fixpoint may apply a rewrite along an equality between types to its recursive argument, which the guard checker accepts because the inductive type is preserved, while the recursive tree recorded for the parameter is altered. A second fixpoint that calls the first inherits the altered recursive tree without verification, so a call that is not structurally decreasing is accepted as terminating. The resulting non-terminating definition proves that a natural number equals its own successor and therefore False, from which any proposition follows. The demonstration uses two axioms that follow from univalence and are consistent with the calculus of inductive constructions, so the contradiction comes from the guard check rather than from the assumptions. A fix is proposed but not merged.	2026-08-24	6.3	CVE-2026-72704
rocq-prover--rocq	The guard checker in Rocq Prover does not follow recursive calls made through a fixpoint's own arguments. A fixpoint may pass itself as a higher-order argument to a second fixpoint, which then applies it to a value that is not a subterm of the structural argument. Passing the recursive function to a plain definition is rejected because the checker unfolds the definition and observes the call, but passing it to a fixpoint is accepted because higher-order recursive calls through fixpoint arguments are not tracked. This admits a type that is definitionally equal to its own negation, so self-application produces False in purely definitional code, without tactics, axioms, plugins or unsafe flags, and Print Assumptions reports the result as closed under the global context. Fixed in Rocq 9.2.0.	2026-08-24	6.3	CVE-2026-72705
rocq-prover--rocq	Rocq Prover does not restore the universe graph's copy of the universe checking flag when a module that locally disabled the check is closed. Local Unset Universe Checking inside a module is expected to last only until the module ends, and the global flag is restored, but the universe graph keeps its own copy which is left disabled. The two views then disagree: Test Universe Checking reports the check as enabled while the kernel continues to accept universe-inconsistent terms. With the constraint between two universes no longer enforced, Hurkens' paradox applies and yields a proof of False, from which any proposition follows. The proof uses no axioms, plugins or unsafe features once the module has closed, and Print Assumptions reports it as closed under the global context, so neither the assumption audit nor the flag query reflects the actual kernel state. No fix is available.	2026-08-24	6.3	CVE-2026-72714
RooCodeInc--Roo-Code	A weakness has been identified in RooCodeInc Roo-Code up to 3.51.1. Affected by this issue is the function ExecaTerminalProcess of the component README File Handler. Executing a manipulation can lead to code injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. Multiple issues were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it."	2026-08-27	6.3	CVE-2026-81834

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This vulnerability only affects products that are no longer supported by the maintainer.			
RooCodeInc--Roo-Code	A flaw has been found in RooCodeInc Roo-Code up to 3.51.1. This issue affects the function path.resolve of the file src/core/tools/ApplyPatchTool.ts of the component ApplyPatchTool. This manipulation causes path traversal. It is possible to initiate the attack remotely. The exploit has been published and may be used. Multiple issues were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it." This vulnerability only affects products that are no longer supported by the maintainer.	2026-08-27	6.3	CVE-2026-81837
RooCodeInc--Roo-Code	A security flaw has been discovered in RooCodeInc Roo-Code up to 3.51.1. Affected by this vulnerability is the function optimizeQuery of the file src/utls/helpers.ts of the component CodeIndexManager. Performing a manipulation results in code injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. Multiple issues were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it." This vulnerability only affects products that are no longer supported by the maintainer.	2026-08-27	5.5	CVE-2026-81833
RooCodeInc--Roo-Code	A security vulnerability has been detected in RooCodeInc Roo-Code up to 3.51.1. This affects the function fetch_instructions of the file malicious_mcp_server.py of the component MCP Integration Trust Model. The manipulation leads to code injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. Multiple issues were reported to the vendor beforehand. They explain, that "they all apply to Roo Code, a project we no longer support - the repository was archived a while ago, and we don't encourage anyone to use it." This vulnerability only affects products that are no longer supported by the maintainer.	2026-08-27	5.5	CVE-2026-81835
roxnor--FundEngine Donation and Crowdfunding Platform	The FundEngine - Donation and Crowdfunding Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wfp_featured_video_url' parameter in all versions up to, and including, 1.8.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The REST endpoint used to submit the video URL has its permission_callback set to __return_true, meaning any authenticated user - including those with Subscriber-level access - can reach the vulnerable code path.	2026-08-25	6.4	CVE-2026-76063
roxnor--FundEngine Donation and Crowdfunding Platform	The FundEngine - Donation and Crowdfunding Platform plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.8.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify arbitrary posts and pages - overwriting title and content, and seizing ownership by supplying an attacker-controlled post_author integer that bypasses wp_kses_post sanitization. The wp_rest nonce required by the handler is trivially obtainable by any logged-in user via /wp-admin/admin-ajax.php?action=rest-nonce and therefore does not constitute an authorization barrier.	2026-08-25	4.3	CVE-2026-75930
roxnor--MetForm Contact Form, Survey, Quiz, Conditional Forms, Form Templates & Custom Form	The MetForm - Contact Form, Survey, Quiz, & Custom Form Builder for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'mf_form_id' Widget Setting in all versions up to, and including, 4.1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload bypasses Elementor's save-time wp_kses_post filter because it contains no HTML	2026-08-25	6.4	CVE-2026-18100

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Builder for Elementor	tags, and MetForm's own str_replace transformation of script tags into JavaScript template literal expressions provides an additional delivery path.			
Ruben Garcia--AutomatorWP	Subscriber Broken Access Control in AutomatorWP <= 5.8.3 versions.	2026-08-24	6.5	CVE-2026-78266
Ruby--resolv	An issue was discovered in the resolv gem before 0.7.2 for Ruby. Resolv::DNS::MessageEncoder wrote a DNS label's length into a single octet without checking its range. A label longer than 255 octets had its length stored modulo 256 but the label data was written unchanged, and thus the bytes on the wire described a different name than the one the application asked to encode. RFC 1035 section 2.3.4 limits a label to 63 octets, and the two high bits of the length octet are reserved for compression pointers. put_string packed the length with put_pack("C", d.length) and put_label used it for labels, and thus any value from 0 to 255 could end up as a label length octet, including the reserved 0x40-0xBF range and the 0xC0-0xFF pointer range. Resolv::DNS::Name.create did not check per-label or total name length either, and thus an attacker-controlled hostname reached the encoder unchanged. An application that resolves an attacker-controlled hostname sends a query whose wire bytes name a domain the attacker chose. A hostname suffix that the application validates against an allowlist becomes padding that never appears on the wire, and thus allowlist and egress checks can be bypassed. The recursive resolver caches the response under the attacker's name, and DNS logs record that name rather than the one the application asked for. A label length whose low octet lands in the 0xC0-0xFF range produces a length octet that conforming parsers read as the start of a compression pointer, with the following attacker-controlled byte as the offset.	2026-08-27	4	CVE-2026-80213
rustdesk--rustdesk	RustDesk versions 1.3.9 through 1.4.9 contain a path traversal vulnerability in the macOS clipboard file-paste code path. The application accepts peer-supplied file descriptor names and joins them to the selected target directory without requiring normalized relative paths. A remote peer in an active clipboard file-paste session can use parent-directory components or absolute paths to write files outside the intended target directory at locations writable by the RustDesk process. Commit 6f1eb16 fixes the issue by validating descriptor names and safely joining paths.	2026-08-26	5.7	CVE-2026-73102
sambitraj--Student Management System	A vulnerability was detected in sambitraj Student Management System up to 56ba287f2e9031523ccb4244cb6e3fe530e4e5d5. Affected by this issue is the function mysqli_query of the file student_dashboard.php of the component Student Dashboard. The manipulation of the argument roll_no results in improper authorization. The attack may be performed from remote. The exploit is now public and may be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-30	6.3	CVE-2026-82553
SciPhi-AI--R2R	R2R through 3.6.5 fails to properly validate user ownership in conversation update and message handlers, allowing authenticated users to modify other users' conversations. Attackers can supply arbitrary conversation identifiers to rename conversations and append messages to other users' conversation histories, corrupting state and injecting malicious content.	2026-08-28	6.5	CVE-2026-82271
Seres Software--syWEB	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Seres Software syWEB allows Reflected XSS. This issue affects syWEB: through 27082026. NOTE: The vendor was contacted and it was learned that the product is not supported.	2026-08-27	6.1	CVE-2026-11747
Seres Software--syWEB	Observable discrepancy vulnerability in Seres Software syWEB allows Account Footprinting. This issue affects syWEB: through 27082026. NOTE: The vendor was contacted and it was learned that the product is not supported.	2026-08-27	5.3	CVE-2026-11754

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
servmask--All-in-One WP Migration Unlimited Extension	The All-in-One WP Migration Unlimited Extension plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ai1wm_backups_path' parameter in all versions up to, and including, 2.84. This is due to insufficient input sanitization and output escaping on user-supplied attributes combined with missing authorization checks on the settings() function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the plugin settings page. The vulnerability was partially patched in version 2.84.	2026-08-28	6.4	CVE-2026-6128
silverstripe--silverstripe-versioned	Silverstripe Versioned provides versioning for Silverstripe models. Prior to 3.2.1, RestoreAction::getRestoreMessage() in src/RestoreAction.php builds ArchiveAdmin restore notifications rendered as CAST_HTML and inserts \$restoredItem->Title, \$restoredItem->URLSegment, \$restoredItem->CMSEditLink(), and \$changedProperty['value'] without applying Convert::raw2xml(). When an administrator restores an archived page containing a crafted title or URL segment, the generated restoration message can execute stored JavaScript in the administrator's browser, compromising the confidentiality and integrity of the CMS session. This issue is fixed in version 3.2.1.	2026-08-28	5.4	CVE-2026-55779
SiteServer--SSCMS	A vulnerability was found in SiteServer SSCMS 7.4.0. Affected by this issue is some unknown functionality of the component Agent Installation Workflow. Performing a manipulation of the argument SecurityKey results in improper access controls. Remote exploitation of the attack is possible. The attack is considered to have high complexity. The exploitation is known to be difficult. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-30	5	CVE-2026-82486
siyuan-note--siyuan	SiYuan before v3.8.1 contains a path traversal vulnerability in the asset.upload MCP tool that accepts arbitrary absolute file paths without workspace boundary validation. Attackers can induce the AI Agent to upload sensitive files such as SSH keys or credentials from outside the workspace into the asset directory through prompt injection.	2026-08-28	5.7	CVE-2026-82233
siyuan-note--siyuan	SiYuan before v3.8.1 fails to filter invisible-tier content from SQL embed blocks, attribute-view keys, and attribute-view backlinks in publish mode. Anonymous readers can enumerate invisible content through these three listing mechanisms despite admin configuration marking content unlisted.	2026-08-30	5.3	CVE-2026-82652
siyuan-note--siyuan	SiYuan 3.8.0 contains a path traversal / sensitive file exposure vulnerability in the RenderTemplate function (kernel/model/template.go), reachable via the POST /api/template/render endpoint (kernel/api/template.go). The endpoint restricts the supplied path only to the workspace directory (util.IsAbsPathInWorkspace) but, unlike the file API's refuseToAccess() blacklist, applies no sensitive-path exclusion. This allows an authenticated attacker to read sensitive workspace files, including conf/conf.json, which contains the API token and cookie signing key. The issue is fixed in v3.8.1.	2026-08-30	4.4	CVE-2026-82650
siyuan-note--siyuan	SiYuan before v3.8.1 does not apply the IsForbiddenAbsPath guard (introduced in GHSA-c8r8-95hg-mp34) to the /history/*path and /repo/diff/*path endpoints in kernel/server/serve.go. These routes require admin authentication but construct file paths independently, so an authenticated administrator can retrieve historical snapshots of sensitive files that the guard is meant to block, including data/.siyuan/publishAccess.json (plaintext publish-mode passwords) and files under data/templates/.	2026-08-30	4.9	CVE-2026-82651
smub--Envira Gallery Image Photo Gallery, Albums, Video Gallery, Slideshows & More	The Envira Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the gallery 'description' configuration field in all versions up to, and including, 1.12.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses a page displaying the gallery with a description enabled.	2026-08-28	6.4	CVE-2026-3423

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Softtr Informatics Technology Trading Limited Company--E-Commerce Pack	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Softtr Informatics Technology Trading Limited Company E-Commerce Pack allows Cross-Site Scripting (XSS). This issue affects E-Commerce Pack: before 5.03.01.49.	2026-08-27	4.3	CVE-2026-5218
SourceCodester--Queue Management System	A flaw has been found in SourceCodester Queue Management System 1.0. This affects an unknown part of the file /api/add_customer.php. This manipulation of the argument Name causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been published and may be used.	2026-08-30	4.3	CVE-2026-82554
sparklemotion--nokogiri	Nokogiri versions before 1.16.5 bundle libxml2 2.12.6, which is affected by CVE-2024-34459 in libxml2's xmlint tool. Nokogiri 1.16.5 upgrades the bundled libxml2 to 2.12.7 to address this. Per the maintainers, there is no impact to Nokogiri users because Nokogiri does not provide or expose the xmlint tool where the issue occurs.	2026-08-25	5.5	CVE-2024-58377
sparklemotion--nokogiri	Nokogiri versions before 1.19.4 contain a possible invalid (out-of-bounds) memory read in the protected internal Node#initialize_copy_with_args helper behind Node#dup and #clone, which unwrapped its source argument as an xmlNode without a type check. If application code calls this protected method with a non-Node argument (e.g., a Namespace), it reads an xmlNs out of bounds, crashing the process. This is only triggerable by a programming error and cannot be triggered by untrusted input or normal use of the public API. Only CRuby is affected. Version 1.19.4 adds a type check and raises TypeError.	2026-08-25	5.5	CVE-2026-79769
sparklemotion--nokogiri	Nokogiri versions before 1.19.3 contain a memory leak in the XSLT Stylesheet transform method when processing Ruby strings containing null bytes. Attackers can exploit this by passing attacker-controlled input with null bytes to transform parameters, causing heap allocations to leak and enabling denial of service against long-running processes.	2026-08-25	5.3	CVE-2026-79771
sparklemotion--nokogiri	Nokogiri versions before 1.19.1 fail to check the return value from xmlC14NExecute in the canonicalize method, returning an empty string on failure instead of raising an exception. Attackers can exploit this to bypass signature validation in downstream SAML libraries by providing invalid canonicalized XML that is incorrectly accepted as valid.	2026-08-25	5.3	CVE-2026-79772
Spring--Micrometer	It is possible for outbound HTTP requests using a Micrometer-instrumented client to cause a denial-of-service (DoS) condition due to an unbounded memory leak. Micrometer 1.17.0 Micrometer 1.16.0 - 1.16.6 Micrometer 1.15.0 - 1.15.12 Micrometer 1.14.0 - 1.14.16 Micrometer 1.9.18 and earlier	2026-08-24	5.9	CVE-2026-59295
Spring--Reactor Core	In Reactor Core, applications that use the Flux.windowTimeout operator with fairBackpressure enabled are vulnerable to a Denial of Service (DoS) condition. Reactor Core 3.8.0 - 3.8.6 Reactor Core 3.5.0 - 3.7.19 Reactor Core 3.4.41 and earlier	2026-08-26	5.9	CVE-2026-47857
Spring--Reactor Core	In Reactor Core, applications that use the Flux.bufferTimeout operator with fairBackpressure enabled are vulnerable to a Denial of Service (DoS) condition. Reactor Core 3.8.0 - 3.8.6 Reactor Core 3.7.19 and earlier	2026-08-26	5.9	CVE-2026-47863
Spring--Reactor Netty	In specific scenarios involving WebSocket handshake redirects to a different origin, the Reactor Netty WebSocket client may leak credentials. In order for this to happen, the HTTP client must have been explicitly configured to follow redirects. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier	2026-08-26	6.1	CVE-2026-47848
Spring--Reactor Netty	In specific scenarios, the Reactor Netty HTTP Server may leak exception details across unrelated requests. In order for this to happen, the server must be	2026-08-26	5.3	CVE-2026-47844

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configured with Brave Tracing. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier			
Spring--Reactor Netty	In specific scenarios, Reactor Netty HTTP Server may incorrectly evaluate the remote IP address when HAProxy Protocol is enabled. In order for this to happen, the application must be configured to use HAProxy Protocol. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier	2026-08-26	5.3	CVE-2026-47845
Spring--Reactor Netty	The vulnerability occurs when a client sends HTTP/1.1 pipelined requests over a single connection, causing the Reactor Netty HTTP server to consume an excessive amount of memory. Reactor Netty 1.3.0 - 1.3.6 Reactor Netty 1.1.0 - 1.2.18 Reactor Netty 1.0.52 and earlier	2026-08-26	5.3	CVE-2026-47874
Spring--Spring AI	ResourceCacheService.getCacheName() builds the on-disk filename by appending the URI fragment verbatim, without stripping path separators or .. sequences, and passes the result to new File(resourceParentFolder, newFileName) before writing the downloaded bytes there. Spring AI 2.0.0 Spring AI 1.1.0 - 1.1.8 Spring AI 1.0.9 and earlier	2026-08-27	5.9	CVE-2026-59294
Spring--Spring AI	RedisChatMemoryRepository.findByMetadata() builds RedisSearch tag and text queries from caller-supplied metadata values without applying RedisSearchUtil.escape(), unlike get(), clear(), and findByTimeRange() in the same class which do escape their inputs. An application that passes user-controlled values to findByMetadata() on a tag-typed metadata field allows an attacker to inject RedisSearch syntax (e.g. x} *) that breaks out of the tag clause and matches all indexed chat messages across every conversation in the index. Spring AI 2.0.0	2026-08-27	4.3	CVE-2026-59319
Spring--Spring AMQP	An attacker who can publish to a queue consumed by an application that has enabled message decompression can crash the consumer JVM with a single ~1 MB message. Spring AMQP 4.1.0 Spring AMQP 4.0.0 - 4.0.4 Spring AMQP 3.2.0 - 3.2.12 Spring AMQP 2.4.18 and earlier	2026-08-26	6.5	CVE-2026-47860
Spring--Spring AMQP	Any application shipping logs to RabbitMQ over TLS via the Log4j2 appender, relying on the documented default, is exposed to man-in-the-middle interception of every log event. Spring AMQP 4.1.0 Spring AMQP 4.0.0 - 4.0.4 Spring AMQP 3.2.0 - 3.2.12 Spring AMQP 2.4.18 and earlier	2026-08-27	6.8	CVE-2026-59272
Spring--Spring AMQP	A single hostile AMQP message can terminate the entire consumer JVM (System.exit(99)), not just the listener thread - full availability loss for every workload co-located in that process. Spring AMQP 4.1.0 Spring AMQP 4.0.0 - 4.0.4 Spring AMQP 3.2.0 - 3.2.12 Spring AMQP 2.4.18 and earlier	2026-08-27	6.6	CVE-2026-59275
Spring--Spring AMQP	When a container-level ErrorHandler is configured (the mitigation for finding 221000), each delivery whose processing throws still permanently consumes one link credit. After initialCredits (default 100) failing messages the receiver's credit reaches zero and the broker stops delivering, leaving the listener silently stalled while isRunning() remains true. Spring AMQP 4.1.0	2026-08-27	6.5	CVE-2026-59320
Spring--Spring AMQP	When the RabbitMQ management aliveness check fails, the configured admin password is embedded in cleartext in the thrown exception message. Spring AMQP 4.1.0 Spring AMQP 4.0.0 - 4.0.4 Spring AMQP 3.2.0 - 3.2.12 Spring AMQP 2.4.18 and earlier	2026-08-27	5.3	CVE-2026-59271
Spring--Spring Batch	Applications that deserialize execution contexts with Jackson2ExecutionContextStringSerializer are vulnerable to a deserialization attack if they use an untrusted data source for the job repository. The JobParameterDeserializer does not properly enforce the trusted-types allowlist, allowing an attacker to craft malicious input that can lead to arbitrary code execution, including known Jackson RCE gadgets. Spring Batch 6.0.0 - 6.0.4 Spring Batch 5.2.0 - 5.2.6	2026-08-27	5.6	CVE-2026-47875

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring Batch	DefaultExecutionContextSerializer, used by default in Spring Batch's JDBC job repository, passes Base64-decoded bytes directly to ObjectInputStream.readObject() without an ObjectInputFilter that restricts types to a trusted class allowlist. Spring Batch 6.0.0 - 6.0.4 Spring Batch 5.2.6 and earlier	2026-08-27	5.6	CVE-2026-47878
Spring--Spring Batch	Spring Batch's FlatFileItemReader supports files where a single logical record spans multiple physical lines - for example, a CSV field that contains embedded newlines wrapped in quotes. A specially crafted input file could exploit the way the reader assembles those multi-line records to consume excessive CPU time and memory, causing the batch job to stall or run out of memory. Spring Batch 6.0.0 - 6.0.4 Spring Batch 5.2.0 - 5.2.6 Spring Batch 4.3.0 - 4.3.13	2026-08-27	5.9	CVE-2026-47881
Spring--Spring Cloud Commons	There is no allow list for property keys when Spring Cloud Commons writable /actuator/env is enabled. Spring Cloud Commons 5.0.0 - 5.0.2 Spring Cloud Commons 4.3.0 - 4.3.3 Spring Cloud Commons 4.0.0 - 4.2.6 Spring Cloud Commons 3.1.10 and earlier	2026-08-27	6.6	CVE-2026-59284
Spring--Spring Cloud Config	Missing Authentication for Critical Function vulnerability in Spring Spring Cloud Config allows Webhook requests to Spring Cloud Config Server's /monitor endpoint are not validated. This issue affects Spring Cloud Config: from 5.0.0 through 5.0.4, from 4.3.0 through 4.3.4, from 4.0.0 through 4.2.8, and through 3.1.14.	2026-08-26	6.8	CVE-2026-47837
Spring--Spring Cloud Config	The Spring Cloud Config Monitor is susceptible to Denial of Service attacks via malicious payloads. Spring Cloud Config 5.0.0 - 5.0.4 Spring Cloud Config 4.3.0 - 4.3.4 Spring Cloud Config 4.0.0 - 4.2.8 Spring Cloud Config 3.1.14 and earlier	2026-08-27	5.3	CVE-2026-59315
Spring--Spring Cloud Config	Spring Cloud Config Server native environment repository allows exposure of configuration files outside of the configured repository path. Spring Cloud Config 5.0.0 - 5.0.4 Spring Cloud Config 4.3.0 - 4.3.4 Spring Cloud Config 4.0.0 - 4.2.8 Spring Cloud Config 3.1.14 and earlier	2026-08-27	4.9	CVE-2026-47894
Spring--Spring Data JPA	Spring Data JPA's Sort validation can be bypassed when parameters containing crafted payload are accepted from untrusted sources. Spring Data JPA 4.1.0 Spring Data JPA 4.0.0 - 4.0.6 Spring Data JPA 3.5.0 - 3.5.13 Spring Data JPA 3.0.0 - 3.4.15	2026-08-26	4.8	CVE-2026-47834
Spring--Spring Data REST	Spring Data REST does not preserve the persisted version (@Version) property of an aggregate root when handling an HTTP PUT against an immutable target type. Spring Data REST 5.1.0 Spring Data REST 5.0.0 - 5.0.6 Spring Data REST 4.5.0 - 4.5.12 Spring Data REST 4.0.0 - 4.4.15 Spring Data REST 3.7.20 and earlier	2026-08-26	4.3	CVE-2026-47850
Spring--Spring for Apache Kafka	JsonKafkaHeaderMapper and DefaultKafkaHeaderMapper include java.net in their default trusted packages list. When these mappers are used - which is the default configuration for all @KafkaListener consumers - an external Kafka producer can inject a java.net.InetAddress type via the spring_json_header_types message header. Spring for Apache Kafka 4.1.0 Spring for Apache Kafka 4.0.0 - 4.0.6 Spring for Apache Kafka 3.0.0 - 3.3.16 Spring for Apache Kafka 2.9.0 - 2.9.14 Spring for Apache Kafka 2.8.12 and earlier	2026-08-27	6.5	CVE-2026-59278
Spring--Spring for Apache Kafka	DeadLetterPublishingRecovererFactory reads the retry_topic-original-timestamp header from an inbound ConsumerRecord and passes its raw bytes directly to new BigInteger(header.value()) with no length or format validation. Spring for Apache Kafka 4.1.0 Spring for Apache Kafka 4.0.0 - 4.0.6 Spring for Apache Kafka 3.0.0 - 3.3.16 Spring for Apache Kafka 2.9.0 - 2.9.14 Spring for Apache Kafka 2.8.12 and earlier	2026-08-27	6.5	CVE-2026-59317
Spring--Spring Integration	Spring Integration's JSON to object conversion uses the json__TypeId__ header to choose the deserialization target type, and resolves that header value to a class with ClassUtils.forName and no type/package allow-list. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	2026-08-26	6.3	CVE-2026-47856

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring Integration	An unauthenticated remote attacker who can send a single UDP packet to a Spring Integration UDP inbound adapter can cause the server to emit an outbound UDP datagram to an arbitrary internal or external host and port of the attacker's choosing. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	2026-08-26	6.3	CVE-2026-47861
Spring--Spring Integration	SerializingHttpMessageConverter deserializes the body of incoming HTTP requests with a raw java.io.ObjectInputStream and no class filtering. Any request with Content-Type application/x-java-serialized-object whose body resolves to a Serializable type is read directly via readObject(). If an application using this converter on an inbound HTTP endpoint has any known Java deserialization "gadget" on its classpath, a remote, unauthenticated attacker can achieve arbitrary code execution. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	2026-08-27	6.4	CVE-2026-47864
Spring--Spring Integration	The UnZipTransformer does not limit decompressed entry size or entry count when processing archives. Consequently, an attacker can send a zip archive that can exhaust JVM heap memory, causing a denial-of-service outage. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	2026-08-27	6.5	CVE-2026-59274
Spring--Spring Integration	Unless the application explicitly raises smbMinVersion, the jCIFS client will negotiate down to SMB1/CIFS, which lacks mandatory signing/encryption and is vulnerable to NTLM relay and content-tampering MITM. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	2026-08-27	6.6	CVE-2026-59293
Spring--Spring Integration	A local unprivileged user on the same host can redirect all Zip/UnZip transformer output into a directory of their choosing by pre-creating /tmp/ziptransformer as a symlink before the application starts. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	2026-08-27	6.8	CVE-2026-59311
Spring--Spring Integration	The EmbeddedHeadersJsonMessageMapper defaults to an overly permissive header parsing posture in its constructor. When decodeNativeFormat processes raw byte payloads, it deserializes embedded JSON headers into a plain Map and constructs a GenericMessage with MutableMessageHeaders without sanitizing or filtering untrusted header names by default. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	2026-08-27	6.3	CVE-2026-59322
Spring--Spring Integration	RFC6587SyslogDeserializer, used by the Spring Integration syslog TCP inbound adapter to decode RFC 6587 / RFC 5424 frames, trusts the sender-supplied octet count of an octet-counted frame and allocates a byte array of exactly that size with no upper bound. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	2026-08-26	5.4	CVE-2026-47859
Spring--Spring Integration	An attacker who can set the file_name header on a message reaching a ZipTransformer with ZipResultType.FILE (the default) can cause the resulting .zip archive to be written to an arbitrary filesystem path outside the configured workDirectory. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12	2026-08-26	5.4	CVE-2026-47862
Spring--Spring Integration	A producer who can publish to a JMS destination consumed by any Spring Integration JMS inbound component can set String JMS properties named replyChannel, errorChannel, or json__TypeId__ which are copied verbatim into the Spring Integration MessageHeaders. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	2026-08-27	5.4	CVE-2026-47880

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring Integration	A single ScriptEngine instance is reused for every message on a script-backed channel. For JSR-223 engines that report THREADING=null (not thread-safe, e.g. the Kotlin kts engine), concurrent message processing can corrupt engine-internal state, potentially leaking one message's payload/headers bindings into another message's script evaluation or throwing spurious exceptions. Spring Integration 7.1.0 Spring Integration 7.0.0 - 7.0.5 Spring Integration 6.5.0 - 6.5.10 Spring Integration 6.4.0 - 6.4.12 Spring Integration 5.5.21 and earlier	2026-08-27	4.2	CVE-2026-59321
Spring--Spring Security	Applications using AesBytesEncryptor with the two-argument constructor or when passing a null IV generator and CBC as the encryption mode encrypt data with AES/CBC using a null (all-zero) initialization vector. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 - 6.5.11 Spring Security 6.4.0 - 6.4.18 Spring Security 5.8.0 - 5.8.27 Spring Security 5.7.0 - 5.7.25	2026-08-26	6.5	CVE-2026-47842
Spring--Spring Security	Several components in Spring Security compare security-sensitive values using standard string equality (String.equals()) rather than a constant-time comparison. Because String.equals() returns as soon as it finds a differing character, the time taken to reject an incorrect value is proportional to the number of leading characters that match the expected value. Spring Security 7.1.0 Spring Security 7.0.0 - 7.0.6 Spring Security 6.5.0 - 6.5.11 Spring Security 6.4.0 - 6.4.18 Spring Security 5.8.0 - 5.8.27 Spring Security 5.7.0 - 5.7.25	2026-08-27	5.9	CVE-2026-59276
StarRocks--starrocks	StarRocks through 4.0.13 contains an information disclosure vulnerability in the query_detail endpoint that returns unfiltered query history for all users. Authenticated attackers with low privileges can access full SQL text, execution plans, and profiling data from every query executed by other users, including statements containing credentials.	2026-08-28	6.5	CVE-2026-82306
StarRocks--starrocks	StarRocks through 4.0.13 contains an authentication bypass vulnerability in five REST handler classes that override execute() directly instead of implementing executeWithoutPassword(). Attackers can access six unauthenticated endpoints on the frontend HTTP port to disclose cluster topology, database metadata, JVM statistics, and version information without credentials.	2026-08-28	5.3	CVE-2026-82276
static-web-server--static-web-server	Static Web Server (SWS) is a production-ready web server suitable for static web files or assets. Through 2.43.0, instances with both basic-auth and metrics features enabled process the /metrics endpoint before the basic-auth check in src/handler.rs, allowing an unauthenticated remote attacker to retrieve Prometheus metrics that disclose virtual host names, request volumes, error rates, latency distributions, and active connections. This issue is fixed in version 2.44.0.	2026-08-26	4.3	CVE-2026-75601
stellarwp--GiveWP Donation Plugin and Fundraising Platform	The GiveWP - Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'give_form' shortcode in all versions up to, and including, 4.14.4. This is due to insufficient input sanitization and output escaping on the continue_button_title and display_style shortcode attributes, which are passed through sanitize_text_field() but not properly escaped when output in HTML data attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-08-28	6.4	CVE-2026-5510
Summit Security Systems--AdisyonPro	Authorization bypass through User-Controlled key vulnerability in Summit Security Systems AdisyonPro allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects AdisyonPro: before v5.21.0.	2026-08-27	6.5	CVE-2026-17562
SUSE--wicked	An out-of-bounds read was found in the DHCPv4 packet capture code of wicked. ni_capture_inspect_udp_header() in src/capture.c reports the IP total length as the payload length instead of the length of the remaining UDP payload. Consequently, the DHCP option walker in the DHCPv4 client (wicked-dhcp4) reads up to ihl + 8 bytes - at most 68 bytes - past the end of the 1500-byte packet receive buffer. An unauthenticated attacker on the same network who sends a crafted DHCP/UDP packet can make the client parse adjacent heap memory as DHCP options, so that	2026-08-27	5.4	CVE-2026-71402

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	heap contents such as allocator metadata or pointer values can be interpreted into lease fields. The over-read is bounded to 68 bytes; no memory write, no attacker control over the adjacent bytes and no remote exfiltration primitive has been demonstrated. This issue affects wicked up to and including version 0.6.80.			
sveltejs--kit	SvelteKit before 2.69.1 fails to properly validate remote form function payload sizes, allowing attackers to crash the Node process by sending large payloads. Repeated exploitation causes denial of service by repeatedly crashing the application process.	2026-08-28	5.3	CVE-2026-82256
sveltejs--kit	SvelteKit versions before 2.69.1 contain a prototype pollution vulnerability in remote form functions with file input fields that accept arbitrary user-controlled path names. Attackers can manipulate the deletion path to remove methods on the prototype, potentially disabling application functionality.	2026-08-28	4.3	CVE-2026-82257
sworddudt--mcp-ffmpeg-helper	A vulnerability was detected in sworddudt mcp-ffmpeg-helper 0.1.0/0.1.1/0.2.1. This affects the function handleToolCall of the file src/tools/handlers.ts of the component Tool Handler. The manipulation of the argument format results in os command injection. Attacking locally is a requirement. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-24	5.3	CVE-2026-78430
Synology--Synology Chat Server	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability in extract domain in Synology Chat Server before 2.4.5-22148 allows remote authenticated users, via a UI interaction, to read or write restricted files and conduct limited denial-of-service attacks in DSM.	2026-08-28	6.5	CVE-2026-9548
Synology--Synology Chat Server	A server-side request forgery (SSRF) vulnerability in webhook in Synology Chat Server before 2.4.5-22148 allows remote authenticated users to obtain non-sensitive information.	2026-08-28	4.3	CVE-2026-9491
tagDiv--tagDiv Composer	The tagDiv Composer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the vc_raw_html shortcode in all versions up to and including 5.4.5. This is due to insufficient input sanitization and output escaping in the vc_raw_html::render() method, which base64-decodes shortcode content (after a strip_tags() that is bypassed because the encoded payload contains no tags on save) and concatenates the result directly into the page HTML. Because WordPress's save-time wp_kses_post() filter only sees the inert base64 text inside a normal shortcode bracket and does not decode it, the dangerous tags survive into post_content and are emitted unescaped at render time. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page (for example, when an Editor or Administrator previews the pending post).	2026-08-25	6.4	CVE-2026-12561
Tammersoft--Shared Files	Contributor Server Side Request Forgery (SSRF) in Shared Files <= 1.7.69 versions.	2026-08-24	6.4	CVE-2026-78269
Tangible--Loops & Logic	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Tangible Loops & Logic.	2026-08-28	6.5	CVE-2026-82123
TanStack--devtools-vite	A vulnerability was found in TanStack devtools-vite 0.7.0. Affected by this issue is the function installPackage of the file packages/devtools-bundler-core/src/package-manager.ts of the component Development Devtools Event Bus. The manipulation of the argument packageName results in os command injection. Attacking locally is a requirement. A high complexity level is associated with this attack. The exploitation is known to be difficult. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-24	4.5	CVE-2026-78177

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
The GNU C Library--glibc	Passing an effectively empty string to the `ccs=` syntax extension of the mode argument in the `fopen` function in the GNU C Library version 2.45 or earlier may result in a heap buffer overflow when the mode string input to the function is attacker controlled. This usage pattern is not seen in applications in common GNU/Linux distributions and applications that process user-supplied values for `ccs` should not pass them through without validation.	2026-08-27	4.9	CVE-2026-18374
themefusion--Avada (Fusion) Builder	The Avada (Fusion) Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'size' Shortcode Attribute in all versions up to, and including, 3.15.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. WordPress's wp_kses_post filter does not neutralize the payload because the injected content resides entirely within a shortcode attribute string containing no HTML angle brackets, causing kses to pass it through unchanged at save time.	2026-08-28	6.4	CVE-2026-16654
ThemeGrill--Magazine Blocks	Contributor Cross Site Scripting (XSS) in Magazine Blocks <= 1.8.6 versions.	2026-08-24	6.5	CVE-2026-78290
themeum--Tutor LMS eLearning and online course solution	The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to Remote Code Execution limited to zero-argument function invocation in all versions up to, and including, 4.0.5 via the tutor_course_filter_ajax AJAX action. This is due to missing authorization on the handler combined with unsanitized array keys being passed to extract() inside tutor_load_template(), allowing attacker-controlled POST data to overwrite the local \$template variable and, in the resulting templates/single-content-loader.php template, the \$method_map and \$context variables invoked at \$method_map[\$context](). This makes it possible for unauthenticated attackers to call an arbitrary zero-argument PHP function server-side and, via WordPress core edit_user(), to create a persistent subscriber-level account from request parameters.	2026-08-28	6.5	CVE-2026-16759
thimpress--LearnPress WordPress LMS Plugin for Create and Sell Online Courses	The LearnPress plugin for WordPress is vulnerable to unauthorized modification of arbitrary WordPress options in versions up to, and including, 4.4.4 via the learnpress_create_page AJAX action. The LP_Admin_Ajax::create_page() handler only checks the edit_pages capability and a wp_rest nonce (both available to Editors), then reads the field_name parameter from the request without restricting it to a learn_press_* allow-list before passing it as the option key to LP_Helper::create_page(), which calls update_option(\$key_option, \$page_id). This makes it possible for authenticated attackers, with Editor-level access and above, to update arbitrary WordPress options to a positive integer (a newly created page ID), enabling actions such as flipping users_can_register to a truthy value to open public registration, corrupting active_plugins to break the site, or otherwise tampering with site-wide settings normally reserved for administrators.	2026-08-25	4.4	CVE-2026-75982
TIM Solutions--TIM Flow	TIM Flow before 26.0.6 contains an improper authorization vulnerability that allows any authenticated user to submit arbitrary SQL queries to a privileged dashboard Excel export endpoint intended for administrative use only. Attackers can craft and submit unauthorized SQL queries to the export endpoint to retrieve sensitive database contents as a downloadable spreadsheet, bypassing role-based access controls.	2026-08-24	6.5	CVE-2026-39914
timescale--pg-aiguide	pg-aiguide started its MCP HTTP transport without enabling the host allow-list the underlying SDK provides. src/httpServer.ts called the shared httpServerFactory helper and never set the DNS-rebinding-protection option, so the transport accepted a request whatever host it named. A page in a browser could therefore point a name it controlled at the address the server was bound to and drive the locally reachable MCP server through the visitor's browser. The protection was already available in the packaged transport and simply not turned on, so updating	2026-08-27	6.8	CVE-2026-81095

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the dependency alone would not have closed it. Version 0.5.1 passes the option explicitly.			
timescale--tiger-gh-mcp-server	tiger-gh-mcp-server started its MCP HTTP transport without enabling the host allow-list the underlying SDK provides. src/httpServer.ts called the shared httpServerFactory helper and never set the DNS-rebinding-protection option, so the transport accepted a request whatever host it named, making the locally reachable GitHub MCP endpoint drivable from a page in a visitor's browser that pointed a name it controlled at the bound address. The fix passes the option explicitly alongside a dependency update; the update alone would not have closed it. The repository has published no release that brackets the fix, so the affected boundary is the commit preceding it.	2026-08-27	6.8	CVE-2026-81100
timescale--tiger-slack	tiger-slack started its MCP HTTP transport without enabling the host allow-list the underlying SDK provides. mcp/src/httpServer.ts called the shared httpServerFactory helper and never set the DNS-rebinding-protection option, so the transport accepted a request whatever host it named, and a page in a browser could point a name it controlled at the address the server was bound to and drive the locally reachable Slack MCP server through the visitor's browser. The fix passes the option explicitly alongside a dependency update; the update alone would not have closed it. The repository publishes no release that brackets the fix, so the affected boundary is the commit preceding it.	2026-08-27	6.8	CVE-2026-81099
twentyhq--twenty	Twenty through 2.35.0 contains an open redirect vulnerability in the OAuthPropagatorController.propagateOAuthCallback endpoint that treats the state query parameter as a redirect URL. Attackers can craft malicious requests to redirect users to arbitrary hosts while forwarding OAuth authorization codes, bypassing domain validation when IS_MULTIWORSPACE_ENABLED is disabled.	2026-08-28	4.7	CVE-2026-82274
ultimatemember--Ultimate Member User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin	The Ultimate Member - User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Textarea Profile Field with HTML Support (DOM Gadget via id Attribute) in all versions up to, and including, 2.12.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is possible because the wp_kses 'templates' allowlist permits the id attribute on div elements but does not neutralize unescaped quotes within its value; when pickdate.js concatenates the stored id value into an HTML string via jQuery .html() on profile page load, the smuggled onfocus and autofocus attribute syntax breaks out of attribute context and executes as JavaScript.	2026-08-25	6.4	CVE-2026-18547
usememos--memos	Memos through 0.30.0 omits the 100.64.0.0/10 carrier-grade NAT address range from SSRF protection in its link-metadata fetcher, allowing unauthenticated attackers to bypass IP validation. Attackers can make the server request internal hosts in that range including cloud metadata services and read page titles and descriptions back.	2026-08-29	5.3	CVE-2026-82476
versatica--mediasoup	mediasoup is a WebRTC video conferencing system. From version 3.20.0 until 3.20.6 for the npm package and from 0.22.0 until 0.22.5 for the Rust crate, mediasoup's built-in SCTP stack authenticates state cookies using only the hardcoded msworker and 0xAD81 magic values instead of a per-instance secret and HMAC, contrary to RFC 9260 Section 5.1.3. The cookie structure and validation in worker/include/RTC/SCTP/association/StateCookie.hpp and worker/src/RTC/SCTP/association/StateCookie.cpp allow an on-path attacker targeting PlainTransport or PipeTransport with SCTP enabled and without DTLS protection to forge a COOKIE-ECHO whose packet verification tag matches the attacker-controlled localVerificationTag. The forged cookie passes StateCookie::IsMediasoupStateCookie() and Association::HandleReceivedCookieEchoChunk(), establishes an unauthorized SCTP association, and permits DataChannel message injection as a trusted peer.	2026-08-25	5.6	CVE-2026-55663

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WebRtcTransport is not affected because its SCTP runs inside DTLS. This issue is fixed in npm version 3.20.6 and Rust crate version 0.22.5.			
vllm-project--vllm	vLLM before 0.27.0 fails to properly classify DeepStream as a GPU backend and omits pixel-limit enforcement in its decode path. Unauthenticated attackers can activate DeepStream at request time to initialize the process-wide GPU decode pool and submit video that bypasses resource controls, causing partial denial of service for concurrent requests.	2026-08-25	5.3	CVE-2026-78684
VMware--Spring Authorization Server	In versions of Spring Authorization Server 1.5.0 through 1.5.7, the authorization endpoint performs insufficient validation of the request_uri parameter. An attacker can craft a request containing an invalid request_uri paired with an unvalidated redirect_uri, which can result in an open redirect to an attacker-controlled site.	2026-08-27	6.1	CVE-2026-59355
Volmarg--personal-management-system	Volmarg Personal Management System contains a path traversal vulnerability that allows authenticated attackers to read arbitrary files by supplying absolute filesystem paths to the GET /public/get-file/{path} endpoint. The path route parameter is passed directly to file_get_contents() without canonicalization against a permitted base directory, enabling attackers to retrieve sensitive files accessible to the PHP-FPM worker process without using directory traversal sequences.	2026-08-27	6.5	CVE-2026-40526
vrana--adminer	Adminer before 5.4.3 inserts unsanitized database server version strings into script tags with valid CSP nonces without proper validation. Attackers controlling a rogue MySQL server can return crafted version strings that break out of the JavaScript context and execute arbitrary code, bypassing Content Security Policy protections.	2026-08-25	6.1	CVE-2026-56704
vrana--adminer	Adminer before 5.4.3 uses a CSRF token scheme that transmits both the XOR mask and the masked value in every token (format (rand XOR secret):rand), allowing anyone who observes a single CSRF token (e.g., via network sniffing, log files, Referrer header, or XSS) to recover the session secret with a single XOR operation and forge unlimited valid tokens. The implementation is further weakened by a low-entropy session token (rand(1,1e6), ~20 bits) that permits blind brute-force, and by use of loose comparison (==) in token verification, enabling PHP type juggling. Exploitation enables cross-site request forgery against authenticated sessions, including execution of arbitrary SQL queries.	2026-08-25	6.8	CVE-2026-56706
vrana--adminer	Adminer before 5.5.0 contains a server-side request forgery vulnerability in the login form's server field validator, which only inspects leading integers for privileged ports and fails to reject non-numeric port values. Attackers can inject PDO DSN keys like host= and port= into the server parameter to bypass the privileged-port restriction and establish TCP connections to arbitrary internal hosts and ports before authentication.	2026-08-25	5.8	CVE-2026-34964
vrana--adminer	Adminer versions 5.3.0 through 5.4.2 with the sql-log plugin enabled contain an arbitrary file write vulnerability in the ns parameter of plugins/sql-log.php. An authenticated user can supply path traversal sequences in the ns parameter to write arbitrary .sql files with attacker-controlled content to any writable directory on the host.	2026-08-25	5.4	CVE-2026-34967
vrana--adminer	Adminer 4.6.0 before 5.5.0 prepends the client-supplied X-Forwarded-Prefix header to \$_SERVER["REQUEST_URI"] with no trusted-proxy check and no validation of the prefix value. An attacker can supply an absolute URL (e.g. X-Forwarded-Prefix: https://evil.example) that flows into Location redirect headers, the Set-Cookie path attribute, and self-referential links. This enables an authenticated open redirect after state-changing POSTs, unauthenticated control of the session cookie path attribute, and poisoning of self-referential links; CR/LF cannot be injected, so header splitting/XSS is not possible.	2026-08-25	4.7	CVE-2026-34959
wagtail--wagtail	Wagtail is an open source content management system built on Django. Prior to versions 7.0.9, 7.3.4, 7.4.3, and 8.0rc2 on their respective release lines, the internal Pages admin API returns page fields declared in api_fields without sufficient access	2026-08-24	4.3	CVE-2026-55468

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	control, allowing a user with Wagtail admin access to retrieve restricted draft and live page content. This issue is fixed in versions 7.0.9, 7.3.4, 7.4.3, and 8.0rc2.			
wallabag--wallabag	wallabag 2 through 2.6.14 allows SSRF because a crafted title or content field is mishandled during PDF export.	2026-08-28	6.4	CVE-2026-82081
wazuh--wazuh	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.14.0 through 4.14.6, a low-privilege API user can read the cleartext cluster key from a configuration endpoint that fails to redact it. The REST API provides a masking control, mask_sensitive_config, that redacts sensitive fields such as authd.pass and cluster.key from configuration responses for users who lack update-config permission, and every config-read endpoint carries this decorator except GET /cluster/local/config. That endpoint, backed by read_config_wrapper, is gated only by cluster:read and returns the local node's cluster configuration including the cleartext key, whereas its siblings return the same value masked. As a result, any account with the default readonly or cluster_readonly role, which is explicitly denied update-config precisely so it cannot view secrets, receives the real cluster key. Because the cluster key authenticates and encrypts traffic between cluster nodes, disclosing it to an unprivileged account provides the authentication precondition for the cluster-peer remote code execution chains established by prior advisories. This issue is fixed in version 4.14.	2026-08-27	6.5	CVE-2026-61802
wazuh--wazuh	Wazuh is an open-source security platform providing unified XDR and SIEM protection for endpoints and cloud workloads. In versions 4.0.0 through 4.14.6, a malicious or man-in-the-middle enrollment manager can crash a Wazuh agent during enrollment by returning a malformed key response with fewer than four fields, causing a NULL pointer dereference. The w_enrollment_process_agent_key() routine splits the manager-provided key into four space-separated fields but does not verify that all fields are present before passing them to validators. Because OS_StrBreak() leaves missing trailing entries as NULL and OS_IsValidName() calls strlen() on its argument without a NULL check, a response such as OSSEC K:'1' reaches OS_IsValidName(NULL) and terminates the agent process. Since Wazuh permits enrollment against an unverified manager when no CA certificate is configured, an attacker operating a rogue manager or intercepting the enrollment flow can deterministically crash agents, resulting in denial of service. This issue is fixed in version 4.14.7.	2026-08-27	5.3	CVE-2026-54084
Webful Creations--RepairBuddy	Unauthenticated Broken Access Control in RepairBuddy <= 4.1223 versions.	2026-08-24	5.3	CVE-2026-78291
WeblateOrg--weblate	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, a user with the built-in "Edit source" role can store a malicious regular expression in a source string's flags that is executed without any timeout, allowing them to stall requests and deny service. Regular expressions supplied through the regex: quality check and regex placeholders are compiled during validation but later run against translation content in RegexCheck and PlaceholderCheck with no time limit, so a catastrophic-backtracking pattern like ^(a aa)+\$ can consume CPU indefinitely. Because Weblate re-runs these checks for every linked target unit in the same request when a source unit's flags change, a single edit can trigger sustained CPU-bound denial of service. This issue is fixed in version 2026.7.	2026-08-26	6.5	CVE-2026-62326
WeblateOrg--weblate	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.8, Weblate's object-scoped RSS feeds do not apply the permission checks used elsewhere, allowing unauthorized users to read change-history metadata from private projects and restricted components. On installations that permit anonymous access, this metadata can be retrieved without any authentication. The exposed information can include project and component identities, contributor usernames and full names, action types, timestamps, and translation or unit links, though translated-string content is not	2026-08-26	5.3	CVE-2026-77507

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	included in the feed. Installations using private projects or restricted components are affected. This issue is fixed in version 2026.8.			
WeblateOrg--weblate	Weblate is a web-based localization tool. In versions prior to 2026.7, several endpoints look up objects in a globally scoped manner rather than restricting the lookup to projects the user can access, so they return HTTP 403 (Forbidden) instead of 404 (Not Found) when a user requests an object they are not authorized to see. This difference lets unauthorized users infer whether a given object exists in a private Weblate project. The issue has been fixed in version 2026.7.	2026-08-26	4.3	CVE-2026-55227
WeblateOrg--weblate	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, a team can require its members to configure two-factor authentication before receiving the team's permissions, but this requirement is not enforced for site-wide global permissions. As a result, a user who belongs to a team that enforces 2FA and grants a global permission still receives that global permission even without 2FA configured, while the same requirement is correctly applied to project-, component-, and workspace-scoped permissions. Such a user can act on the granted global permission, including reaching the site management interface at /manage/. This issue is fixed in version 2026.7.	2026-08-26	4.4	CVE-2026-61790
WeblateOrg--weblate	Weblate is a web-based continuous localization platform used to manage software translations. In versions prior to 2026.7, an authenticated user with access to a project can retrieve the change history of restricted components in that project through nested API change endpoints, even without permission to view those components directly. The nested endpoints do not apply the component-level access checks enforced on the direct component views, so the requester can enumerate changes for components that should be hidden from them. The exposed data can include the restricted component's identity, translation and unit links, and change payload fields such as source or translated string content in the target, old, and details values. This issue is fixed in version 2026.7.	2026-08-26	4.3	CVE-2026-62249
wedevs--WP Project Manager Pro	The WP Project Manager Pro plugin for WordPress is vulnerable to SQL Injection in all versions up to, and including, 4.0.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-25	6.5	CVE-2026-78470
wger-project--wger	A flaw has been found in wger-project wger up to 2.6.0-alpha2. This issue affects the function reset_user_password of the file wger/gym/views/gym.py of the component Password Reset. Executing a manipulation can lead to cross-site request forgery. It is possible to launch the attack remotely. This patch is called 3c6ce4b7f3eeafeb35318c6c4e82b1a3fd28b314. It is advisable to implement a patch to correct this issue.	2026-08-30	4.3	CVE-2026-82544
wintercms--winter	Winter CMS is a content management system built on the Laravel PHP framework. In versions up to and including 1.2.12, the CMS section's Theme Editor AJAX handlers did not enforce per-template-type permission checks, allowing a backend user with any single CMS permission to act on template types outside their authorized scope. The CMS controller gated access to the section as a whole using OR-logic across its five permissions, but individual handlers such as onSave(), onDelete(), and onDeleteTemplates() did not verify that the user held the specific permission for the requested template type, so a user with only cms.manage_pages could craft AJAX requests to delete layouts, modify partials, or read content files. Separately, the AssetList widget was registered for any user who passed the controller gate regardless of the cms.manage_assets permission, and its onUpload() handler omitted the theme-validation call present on the other mutating handlers, permitting unauthorized file uploads into the active theme's	2026-08-26	6.8	CVE-2026-32639

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	asset directory. Exploitation requires an authenticated backend account holding at least one of the CMS Theme Editor permissions. This issue is fixed in version 1.2.13.			
wintercms--winter	Winter CMS is a content management system built on the Laravel PHP framework. In versions up to and including 1.2.12, the backend Filter widget is vulnerable to SQL injection through the numberrange scope type when that scope is configured with a conditions key, allowing an authenticated backend user to inject arbitrary SQL. The scope's filter values are interpolated into the conditions statement without parameter binding, so a user with access to a list view whose filter uses this scope and configuration can supply crafted input through the filter's AJAX handler and read arbitrary database contents. No built-in Winter CMS backend views use this scope type and configuration combination, so exploitation requires a third-party plugin to have registered a numberrange filter scope with a conditions key, and a vanilla installation without such plugins is not affected. This issue is fixed in version 1.2.13.	2026-08-26	5.9	CVE-2026-32593
wintercms--winter	Winter CMS is a content management system built on the Laravel PHP framework. In versions up to and including 1.2.12, the backend FileUpload form widget trusted an attacker-controlled file_id POST parameter when resolving the attachment it operates on, allowing an authenticated backend user to read and modify attachment records belonging to other users or records. The widget's getFileRecord() lookup resolved the posted id against the global system_files table without verifying that the file belonged to the widget's own relation, parent record, or deferred-binding session. Because all attachments share a single File model and table and attachment ids are sequential integers that are easily enumerated, a user reaching any form with a fileupload field, including the built-in My Account avatar field that requires no specific permission, could target arbitrary attachments to modify their title and description via onSaveAttachmentConfig and change their sort order via onSortAttachments, which passed posted ids straight to an unscoped update. CSRF tokens remain enforced, so exploitation requires a valid authenticated backend session with any level of access. This issue is fixed in version 1.2.13.	2026-08-26	5.4	CVE-2026-54256
wintercms--winter	Winter CMS is a content management system built on the Laravel PHP framework. In versions up to and including 1.2.12, authenticated backend users can disclose arbitrary files readable by the PHP process by injecting @import (inline) directives into LESS source that the backend compiles, because the LESS parser was instantiated without a safe import resolver and fell back to the raw attacker-supplied path when no allowed root matched. The flaw is reachable through four entry points that share the same root cause: the Brand Settings custom_css field, the Editor Settings html_custom_styles field, the Mail Brand Settings colour-picker fields whose values are concatenated into LESS source without escaping, and theme .less, .sass, and .scss assets compiled when served. Both absolute paths and .. traversal outside the asset's own tree were accepted, so an attacker could read any file the web process can access, most significantly the application .env file and the APP_KEY and database credentials it contains. Exploitation requires a backend account holding one of the associated permissions, which are assigned by default to the built-in Developer role. This issue is fixed in version 1.2.13.	2026-08-26	4.9	CVE-2026-63179
wintercms--winter	Winter CMS before 1.2.13 contains a local file inclusion vulnerability in the JavascriptImporter filter that allows authenticated users with cms.manage_assets permission to disclose arbitrary server-readable files by placing =include or =require directives in theme JavaScript assets. Attackers can reference files like .env outside the theme directory, and the combined output served through the combine route becomes readable by unauthenticated visitors, exposing application keys and database credentials.	2026-08-25	4.9	CVE-2026-79773
wolfSSL Inc.--wolfEngine	wolfEngine before 1.4.1 sources the explicit AES-CCM nonce for TLS 1.2 and DTLS 1.2 records from the record input buffer instead of the TLS sequence number carried in the additional authenticated data. Because the record layer leaves the explicit-nonce field for the cipher to populate, the value read is constant across	2026-08-28	6.5	CVE-2026-81341

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	records, so every AES-CCM record within a connection is encrypted under an identical key and nonce pair. Reusing a CCM key and nonce weakens confidentiality (identical keystream across records, so a known record recovers the others) and integrity (authentication tag forgery). Only wolfEngine is affected; wolfProvider is not. AES-GCM under wolfEngine is tracked separately. AES-CCM cipher suites are not enabled by default and must be explicitly selected, which limits exposure. TLS 1.3 and non-TLS use of the cipher are not affected.			
WP Chill--Kali Forms	Unauthenticated Broken Access Control in Kali Forms <= 2.4.23 versions.	2026-08-27	5.3	CVE-2026-81276
WP Manage Ninja--Fluent Boards Pro	Subscriber Cross Site Scripting (XSS) in Fluent Boards Pro <= 2.0.11 versions.	2026-08-27	6.5	CVE-2026-78273
WP Manage Ninja--Fluent Boards Pro	Editor Arbitrary File Deletion in Fluent Boards Pro <= 2.0.11 versions.	2026-08-27	6.8	CVE-2026-78275
WP Manage Ninja--FluentPlayer Pro	Editor Broken Access Control in FluentPlayer Pro <= 1.3.2 versions.	2026-08-27	4.9	CVE-2026-81272
WP ManageNinja LLC--Fluent Boards Pro	Subscriber Insecure Direct Object References (IDOR) in Fluent Boards Pro <= 2.0.11 versions.	2026-08-24	5.3	CVE-2026-78278
WP ManageNinja LLC--Fluent Support Pro	Subscriber Broken Access Control in Fluent Support Pro <= 2.3.1 versions.	2026-08-24	5.4	CVE-2026-78272
WP ManageNinja LLC--Fluent Support Pro	Unauthenticated Cross Site Request Forgery (CSRF) in Fluent Support Pro <= 2.3.1 versions.	2026-08-24	5.4	CVE-2026-78279
WP ManageNinja LLC--FluentCRM Pro	Subscriber Server Side Request Forgery (SSRF) in FluentCRM Pro <= 3.1.12 versions.	2026-08-24	4.9	CVE-2026-78277
wpcreatix--Media Sweep WordPress Media Cleaner	The Media Sweep - WordPress Media Cleaner plugin for WordPress is vulnerable to generic SQL Injection via the 'fields' parameter in all versions up to, and including, 1.1.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-08-25	4.9	CVE-2026-77824
WPDeveloper--Essential Addons for Elementor	Authentication Bypass by Spoofing vulnerability in WPDeveloper Essential Addons for Elementor allows Identity Spoofing. This issue affects Essential Addons for Elementor: from n/a through 6.8.0.	2026-08-28	5.3	CVE-2026-81777
wpdevteam--BetterLinks Link Shortener, Link Cloaking, Redirects, Affiliate Link Manager & MCP	The BetterLinks - Link Shortener, Link Cloaking, Redirects, Affiliate Link Manager & MCP plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.1.0. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary BetterLinks short URLs with attacker-controlled slugs and redirect destinations, enabling phishing and SEO abuse. Exploitation requires the Fluent Boards companion plugin to be installed and active (so that the FLUENT_BOARDS constant is defined), and is further facilitated by the betterlinks_admin_nonce nonce being emitted on every frontend page via wp_localize_script, making it accessible to any authenticated user.	2026-08-25	4.3	CVE-2026-19801
wpeverest--Everest Forms Contact Form, Payment Form,	The Everest Forms plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 3.4.4. This is due to the 'load_previous_field_value()' method in 'class-evf-form-task.php' accepting arbitrary URL values from '\$_POST' data for upload fields without domain	2026-08-28	5.3	CVE-2026-5096

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Quiz, Survey & Custom Form Builder with AI	restriction, which are then passed to `wp_remote_head()` in the `get_local_file_size()` method of `class-evf-form-fields-upload.php`. This makes it possible for unauthenticated attackers to force the WordPress server to make outbound HTTP HEAD requests to arbitrary URLs by submitting a form with an upload field containing a malicious URL while leaving a required field empty to trigger form re-rendering.			
wpmet--ElementsKit Pro	The ElementsKit Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 's' parameter of the Advanced Search REST endpoint in all versions up to, and including, 4.10.1 due to insufficient input sanitization and output escaping. The REST endpoint at /wp-json/elementskit/v1/advanced-search uses permission_callback set to __return_true, allowing unauthenticated access. Search terms are stored in the ekit_advanced_search_popular_keyword WordPress option via update_option(). While sanitize_text_field() is applied, it does not encode double quotes, and the stored keywords are rendered in HTML attributes via sprintf without esc_attr(), allowing attribute injection. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user triggers the "no results" popular keywords view on pages using the Advanced Search widget.	2026-08-28	6.1	CVE-2026-4246
WPMU DEV--Forminator	Unauthenticated Other Vulnerability Type in Forminator <= 1.57.1 versions.	2026-08-28	5.3	CVE-2026-82220
wpsoul--Greenshift animation and page builder blocks	The Greenshift - animation and page builder blocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the customapi action handler in versions up to, and including, 12.8.9. This is due to insufficient sanitization of API responses before output via innerHTML. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page.	2026-08-26	6.4	CVE-2026-5092
WWBN--AVideo	WWBN AVideo contains an unauthenticated credential submission vulnerability in plugin/Live/api/preauthorize.json.php that accepts credentials over GET without rate limiting. Attackers can submit correct credentials repeatedly to trigger uncapped two-factor confirmation emails and perform sustained password guessing attacks against user accounts.	2026-08-30	6.5	CVE-2026-82643
WWBN--AVideo	WWBN AVideo contains an unauthenticated reflected cross-site scripting vulnerability in the url2Embed.json.php endpoint that allows attackers to inject malicious scripts by supplying URLs with HTML metacharacters. Attackers can mint an encrypted evideo payload containing unescaped markup, then deliver it as a legitimate-looking link on the site's own domain to execute JavaScript in victims' sessions and steal cookies or CSRF tokens.	2026-08-30	6.1	CVE-2026-82646
WWBN--AVideo	WWBN AVideo contains a cross-site request forgery vulnerability in sendEmail.json.php that allows authenticated administrators to send mail from the site's contact address by bypassing origin checks and captcha validation. Attackers can craft a malicious web page that, when visited by an authenticated admin, sends emails with attacker-controlled subject and body to arbitrary recipients, passing SPF/DKIM/DMARC validation for phishing and brand impersonation attacks.	2026-08-30	6.1	CVE-2026-82647
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs WebSocket subscription handlers fail to enforce the privileges required by equivalent REST endpoints. PacketsApi.subscribePackets exposes the packets WebSocket topic without ObjectPrivilegeType.ReadPacket, ProcessingApi.subscribeAlgorithmStatus exposes the algorithm-status WebSocket topic without ObjectPrivilegeType.ReadAlgorithm, and MdbOverrideApi.subscribeMdbChanges exposes the mdb-changes WebSocket topic without SystemPrivilege.GetMissionDatabase. A low-privilege authenticated user can receive telemetry packets, algorithm status, and mission database change	2026-08-28	6.5	CVE-2026-55545

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	information outside the assigned authorization scope. This issue is fixed in versions 5.12.8 and 5.13.2.			
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.9.4, Yamcs reflects an attacker-controlled redirect_uri parameter from GET /auth/authorize into yamcs-core/src/main/resources/auth/templates/authorize.html without adequate HTML escaping by yamcs-core/src/main/java/org/yamcs/http/auth/AuthHandler.java and yamcs-core/src/main/java/org/yamcs/http/HandlerContext.java. A crafted authorization URL can execute JavaScript when opened by a Yamcs user. The script can access browser-held authentication material and transmit it to an attacker, enabling account compromise. This issue is fixed in version 5.9.4.	2026-08-28	6.5	CVE-2026-55549
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs omits SystemPrivilege.ControlAccess checks from lamApi.listRoles, lamApi.getRole, and lamApi.listPrivileges in yamcs-core/src/main/java/org/yamcs/http/api/lamApi.java. Any authenticated account can call GET /api/roles, GET /api/roles/{name}, and GET /api/privileges to enumerate available system privileges and configured role mappings. The disclosure reveals security configuration that can support targeted privilege-escalation attempts. This issue is fixed in versions 5.12.8 and 5.13.2.	2026-08-28	4.3	CVE-2026-55547
yamcs--yamcs	Yamcs is a mission control framework. Prior to 5.12.8 and 5.13.2, Yamcs processes attacker-controlled data from the /ext URL route in yamcs-web/src/main/webapp/projects/webapp/src/app/core/routes/extension.matcher.ts, extension.component.ts, and app.component.ts without checking registered plugin IDs before DOM rendering through innerHTML. A crafted URL can execute JavaScript when opened by a user. The script can read data available to the Yamcs web application and perform actions in the user context. This issue is fixed in versions 5.12.8 and 5.13.2.	2026-08-28	4.3	CVE-2026-55566
zackees--transcribe-anything	A flaw has been found in zackees transcribe-anything up to 4.1.0. Affected is the function ytdlp_download of the file src/transcribe_anything/ytdlp_download.py of the component Yt-dlp Download. This manipulation of the argument url causes os command injection. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is told to be difficult. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-25	5.6	CVE-2026-79792
zephyrproject--zephyr	The Zephyr ext2 filesystem driver fails to validate the s_log_block_size field of the on-disk superblock when mounting a filesystem. ext2_verify_disk_superblock() in subsys/fs/ext2/ext2_impl.c checks the magic number, revision, inode size and group counts, but never bounds s_log_block_size. On a successful verify, subsys/fs/ext2/ext2_ops.c computes fs->block_size = 1024 << superblock.s_log_block_size from this attacker-controlled uint32_t, so a crafted value either overflows the shift (undefined behaviour) or yields a block size far larger than CONFIG_EXT2_MAX_BLOCK_SIZE. That block size is then passed to k_mem_slab_init() by ext2_init_blocks_slab() to carve CONFIG_EXT2_MAX_BLOCK_COUNT blocks out of the fixed static buffer __ext2_block_memory_buffer, whose size is CONFIG_EXT2_MAX_BLOCK_COUNT * CONFIG_EXT2_MAX_BLOCK_SIZE. k_mem_slab_init() does not verify that the requested blocks fit the buffer, and the ext2 wrapper discards its return value, so the slab is laid out past the end of the static buffer. The mount immediately reads block-group, bitmap and inode blocks of fs->block_size bytes each into these slab blocks, producing an out-of-bounds write into adjacent static memory on the first block read. The entire path is gated only by data read from the mounted image, making this reachable by any attacker who can present a crafted ext2 image to a device that mounts it (for example a removable SD card or storage medium). Because the ext2 driver runs in kernel mode, supplying image bytes yields a supervisor-mode memory-corruption primitive, with impact ranging from denial of service to potential code execution. The fix rejects s_log_block_size values that overflow the shift (greater than 11) or that produce a block size exceeding	2026-08-25	6.8	CVE-2026-13215

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CONFIG_EXT2_MAX_BLOCK_SIZE, so the block slab can no longer be initialized larger than its backing buffer.			
zephyrproject--zephyr	The virtio PCI driver (drivers/virtio/virtio_pci.c) parses a device's PCI capability list during driver initialization. In virtio_pci_read_cap() the device-supplied capability length byte cap_len (read from PCI config space via pcie_conf_read()) was only checked with assert(tmp.cap_len == cap_struct_size). That assert resolves to __ASSERT_NO_MSG(), gated by CONFIG_ASSERT, which defaults off in production builds, so the value reached the copy logic completely unvalidated. The length then drives a loop that copies extra capability dwords into a fixed-size stack buffer supplied by the caller. A cap_len below the 24-byte base struct virtio_pci_cap underflows the unsigned extra_data_words count to a near-SIZE_MAX value, producing an effectively unbounded stack write; a cap_len above the caller's buffer (up to 255) writes up to roughly 228 bytes of device-controlled data past the buffer. Both are out-of-bounds writes of attacker-controlled content executed in kernel mode during boot-time device probe. The input originates from the virtio device. In the common deployment where Zephyr runs as a guest under a hypervisor, the device backend is the host, which already fully outranks the guest, so the bug yields no privilege escalation. The exploitable case is a virtio device that is untrusted relative to the Zephyr kernel - an untrusted or physical/passthrough virtio PCIe device on a bare-metal system, or a confidential-computing posture where the guest must defend against the host - where a malicious device can corrupt the kernel stack and potentially achieve code execution or a crash. The fix replaces the compiled-out assert with a runtime range check rejecting cap_len outside [sizeof(struct virtio_pci_cap), cap_struct_size] before any arithmetic or copy.	2026-08-25	6.1	CVE-2026-13216
zephyrproject--zephyr	Zephyr's WireGuard VPN data-plane receive handler wg_process_data_message() in subsys/net/lib/wireguard/wg_crypto.c validated the anti-replay counter too late. After AEAD decryption of a MESSAGE_TRANSPORT_DATA packet succeeded, the code committed several peer-state changes - update_peer_addr() (endpoint roaming update), the keypair->last_rx/peer->last_rx liveness timers, and keypair_update() (promote nex-current and destroy the previous keypair) - and only afterward called wg_check_replay(). On a replayed packet the replay check returned -EINVAL, but none of the preceding mutations were rolled back. The AEAD tag authenticates content but not freshness, so a replayed-but-authentic transport packet decrypts correctly. An attacker who captures one valid ciphertext off the wire (an on-path or shared-medium observer) can re-inject it from an arbitrary spoofed source address. Reaching the handler requires no credentials: it is driven directly from inbound UDP datagrams via the dispatch in subsys/net/lib/wireguard/wg.c. Because the state mutations committed before the replay check, the replay repoints the peer endpoint to the attacker-chosen source address (roaming hijack), redirecting the victim's subsequent outbound tunnel traffic until the legitimate peer's next packet re-corrects it; it also prematurely destroys the previous keypair and refreshes the RX liveness timer. The tunnel payload stays encrypted under the session keypair, so this is an integrity/availability impact (traffic redirection and session disruption), not payload disclosure. The fix moves wg_check_replay() to immediately after a successful decrypt, before any peer-state mutation, matching the WireGuard specification and the Linux reference implementation.	2026-08-28	6.5	CVE-2026-13734
zephyrproject--zephyr	The userspace syscall verifier z_vrfy_mbox_send() in drivers/mbox/mbox_handlers.c validated the nested msg->data/msg->size fields by reading them directly out of live userspace memory, and then forwarded the original, still-mutable userspace struct mbox_msg * pointer to z_impl_mbox_send() and the underlying driver. Between the access check and the driver's use of msg->data, the validated pointer could be replaced, leaving a time-of-check/time-of-use window. On a system built with CONFIG_USERSPACE, any unprivileged userspace thread may invoke the mbox_send() system call. A second thread sharing the caller's address space can race to overwrite msg->data with a	2026-08-24	6.4	CVE-2026-9728

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	supervisor (kernel) address after the verifier's bounds check has passed but before the driver dereferences it. The driver then reads from the attacker-chosen address in supervisor context (for example memcpy(&data32, msg->data, msg->size) in the NXP mailbox driver, whose bytes are subsequently emitted to the peer mailbox endpoint). The impact is a userspace-to-supervisor access-control bypass: disclosure of kernel memory contents (high confidentiality impact), or, for an invalid/unmapped target address, a faulting kernel read causing denial of service. The fix snapshots the entire struct mbox_msg into a kernel-stack copy with k_usermode_from_copy() and validates and forwards that immutable copy, closing the race.			
zephyrproject--zephyr	The Hearing Access Service (HAS) GATT server in subsys/bluetooth/audio/has.c installs a connection-callback set unconditionally via BT_CONN_CB_DEFINE, so security_changed() runs for every connection that establishes security even before the application has called bt_has_register(). The service attribute pointers hearing_aid_features_attr, preset_control_point_attr, and active_preset_index_attr remain NULL until bt_has_register() resolves them and sets has.registered. With CONFIG_BT_SETTINGS, settings_set_cb() restores each bonded client's persisted context at boot and unconditionally sets context->flags to BONDED_CLIENT_INIT_FLAGS (non-zero). When a previously bonded peer reconnects and re-establishes security during the startup window before bt_has_register() has been called, security_changed() sees the non-zero flags and schedules notify_work_handler, which calls bt_gatt_is_subscribed() with a still-NULL attribute pointer. That triggers an assertion (__ASSERT(attr, ...)) in bt_gatt_is_subscribed(), or a NULL dereference of attr->uuid when assertions are compiled out. The result is a remotely triggerable (Bluetooth, adjacent) crash of the HAS peripheral. Exploitation requires the peer to have previously bonded with the device and to reconnect within the boot-time race window before the application registers the service; a peer that reconnects persistently can prolong the outage. Impact is denial of service only, with no memory corruption or information disclosure. The fix adds an early if (!has.registered) { return; } guard in security_changed(), so no notification work is scheduled until the GATT service is registered and its attribute pointers are valid.	2026-08-24	5.3	CVE-2026-13213
zephyrproject--zephyr	The OCPP 1.6 client in subsys/net/lib/ocpp/ocpp.c reconstructs a session handle and PDU id from the uid field of a CALLRESULT message. In ocpp_process_server_msg() the code calls atoi(strtok_r(uid, "-", &tmp)) without checking the strtok_r return value. When the server-supplied uid is empty or contains no - delimiter, strtok_r() returns NULL and atoi(NULL) dereferences a NULL pointer, which is undefined behaviour. The uid originates from network data: parse_rpc_msg() in subsys/net/lib/ocpp/ocpp_j.c JSON-parses a frame received from the OCPP central system over TCP/WebSocket and copies the server-controlled string into the local buffer. A malicious or compromised central system, or a man-in-the-middle on a non-TLS ws:// connection, can return a malformed uid to reach the defect. No authentication beyond the existing server connection (or MITM position) is required, and the reconstructed pointer is membership-validated by ocpp_session_is_valid(), so the impact is limited to the NULL dereference rather than arbitrary pointer use. On Zephyr targets that trap access to address 0 (MMU/MPU platforms or CONFIG_NULL_POINTER_EXCEPTION_DETECTION), the dereference faults inside the OCPP reader thread and invokes the fatal handler, producing a remote denial of service of the charge point; on bare targets where address 0 is readable the call returns 0 and is benign, so the impact is availability-only and platform-conditional. The applied fix guards only the first atoi(); the second strtok_r(NULL, "-", &tmp) followed by pdu = atoi(buf) in the same function remains unguarded and the identical NULL dereference is still reachable from the same network input when the uid has a first token but no second --delimited token. A complete fix should validate the second token as well.	2026-08-25	5.9	CVE-2026-13217

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zephyrproject--zephyr	The UMP Stream responder library in lib/midi2/ump_stream_responder.c builds reply packets in a 16-byte struct midi_ump (uint32_t data[4]). The builders make_endpoint_info() and make_function_block_info() populate only the first two words (res.data[0] and res.data[1]) and, before this fix, declared their result as an uninitialised local (struct midi_ump res;). The remaining two words (res.data[2], res.data[3]) retain stale stack contents. Endpoint Info and Function Block Info notifications are UMP Stream messages (UMP_MT_UMP_STREAM), which are 4 words long, so the full 16-byte packet - including the two uninitialised words - is transmitted verbatim by cfg->send(). The responder is driven by attacker-supplied UMP Stream Endpoint-Discovery / Function-Block-Discovery requests via ump_stream_respond(). In the in-tree Network MIDI 2.0 server (subsys/net/lib/midi2/netmidi2.c) these requests arrive as UDP datagrams and, with the default no-authentication endpoint, a remote peer can establish a session and trigger the responses; the same library also serves USB MIDI 2.0 hosts. Each discovery request causes the device to disclose 8 bytes of its own uninitialised stack memory to the peer, and the request is freely repeatable. This is a confidentiality-only information leak (root cause is use of an uninitialised variable, CWE-457/CWE-908); the leaked words could include residual data or pointer values. There is no memory-corruption, integrity, or availability impact. The fix zero-initialises both result structs (struct midi_ump res = {0};), so the trailing words are cleared before transmission. These are the only two responder builders that left trailing words unset (send_string() already zeroes its buffer), so the leak is fully closed.	2026-08-24	5.3	CVE-2026-13343
zephyrproject--zephyr	The Zephyr ext2 filesystem driver validates the on-disk block bitmap in ext2_init_fs() (subsys/fs/ext2/ext2_impl.c) by passing fs_blocks = s_blocks_count - s_first_data_block to ext2_bitmap_count_set(). That helper (subsys/fs/ext2/ext2_bitmap.c) treats its argument as a number of bits and reads one bitmap byte per eight bits, but the bitmap buffer (BGROUP_BLOCK_BITMAP) is a single fetched block of only fs->block_size bytes (capacity fs->block_size * 8 bits). s_blocks_count and s_first_data_block are taken verbatim from the superblock and were never bounded against this single-group capacity; ext2_verify_disk_superblock() checks the magic, revision, and block-size shift but not the block count. A crafted ext2 image with an oversized s_blocks_count (up to ~4 billion, against a maximum 4096-byte block / 32768-bit bitmap) makes ext2_bitmap_count_set() scan roughly 512 MB of memory past the bitmap block - a large out-of-bounds read of the static block slab and adjacent memory. The defect is reached during mount: ext2_init_fs() is invoked from ext2_mount() (subsys/fs/ext2/ext2_ops.c), the registered .mount operation. Any path that mounts an attacker-supplied ext2 image (removable media, a disk/flash partition, or a downloaded image) triggers it. The kernel-privileged parser operates on attacker-controlled data, so the bug is exploitable wherever untrusted ext2 media can be mounted. Impact is an out-of-bounds read only: the resulting bit count is compared internally and the mount is rejected, so no attacker-controlled bytes are returned (not a useful information leak). The ~512 MB over-read will almost certainly cross an unmapped or MPU-protected boundary and fault, crashing the system - a denial of service triggered by mounting a single malformed image. The fix rejects any image whose fs_blocks exceeds fs->block_size * 8 before the scan.	2026-08-25	5.5	CVE-2026-13478
zephyrproject--zephyr	The IEEE 1588 PTP management-message parser in subsys/net/lib/ptp/tlv.c mishandles the PTP_MGMT_TIME management id. In tlv_mgmt_post_rcv(), the PTP_MGMT_TIME case casts mgmt_tlv->data to a 10-byte struct ptp_timestamp and reads it (then byte-swaps and writes it back) without first checking that the TLV data field is at least sizeof(struct ptp_timestamp). Every sibling management id in the same switch validates its length first; PTP_MGMT_TIME was the only case lacking that check. The length passed in is the management data size (tlv->length - 2), and the upstream guard in ptp_tlv_post_rcv() only requires tlv->length > 2, while msg_tlv_post_rcv() validates only that the TLV fits within the received byte count, not a per-id minimum. A peer on the local PTP segment can therefore send a PTP_MSG_MANAGEMENT message carrying a short PTP_MGMT_TIME TLV (data	2026-08-26	5.4	CVE-2026-13481

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	as small as 2 bytes), causing the parser to read and write 8 bytes beyond the validated data. The message type and TLV contents are taken straight off the wire, so the path is reachable by any adjacent attacker when CONFIG_PTP is enabled. The over-read and write-back stay within the struct ptp_msg allocation (mgmt_tlv->data lives in the leading mtu[NET_ETH_MTU] union member, so data + 10 lands at most a few bytes past mtu[], inside the same object), so this is an out-of-bounds read of adjacent in-object memory plus a bounded in-place corruption of the message's parsed timestamp, not past-allocation memory corruption. Impact is limited to minor information exposure of adjacent bytes and corruption of the device's parsed management TIME value; there is no crash on the access and no reachable reference-count corruption. The fix adds if (length < sizeof(struct ptp_timestamp)) { return -EBADMSG; } before the cast, matching the other management-id cases and fully closing the receive-path defect.			
ZLMediaKit-- ZLMediaKit	ZLMediaKit confines the downloadFile API to a configured set of root directories with a prefix comparison that does not account for directory boundaries. The configuration loader in server/WebApi.cpp builds each root with File::absolutePath("", item, true); because the relative-path argument is empty that helper returns the value without a trailing separator. The handler then accepts a requested path when start_with(file_path, root) holds, so a sibling directory whose name merely begins with the configured root string satisfies the test and is served. The only other guard rejects a path containing two dots, which this requires none of. The equivalent confinement check for the ordinary static file server in src/Http/HttpFileManager.cpp computes its root with a non-empty second argument, which appends the separator before comparing, and so is not affected. The endpoint requires the configured API secret, so this grants no privilege beyond what that secret already implies, but it reads files outside the directory the operator confined it to, and the reference container runs the server as root.	2026-08-26	4.9	CVE-2026-81028
ZTE--SCP	With legitimate user credentials in hand, attackers can construct malicious SQL statements to bypass authentication logic and execute arbitrary database queries directly. This will consequently lead to slow database queries and expanded query coverage. This vulnerability features a low exploitation threshold, wide scope of impact, requires no external privilege escalation, and is classified as a high-priority fix.	2026-08-26	6.3	CVE-2026-9668

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Baserow--Baserow	A security flaw has been discovered in Baserow up to 2.3.2. Affected by this issue is the function BaserowImpersonateAuthTokenSerializer of the file backend/src/baserow/api/admin/users/serializers.py of the component Inactive Non-Staff User Handler. Performing a manipulation results in improper authorization. Remote exploitation of the attack is possible. The complexity of an attack is rather high. The exploitation is known to be difficult. The presence of this vulnerability remains uncertain at this time. Upgrading to version 2.3.3 can resolve this issue. The affected component should be upgraded. The project maintainer explains: "While the problem exists, I'm not really sure if it's a vulnerability. (....) Even though the back gives a token for a deactivate user, none of the endpoints actually work. That said, we will fix it, but so far it seems more like a bug instead of a vulnerability."	2026-08-04	2.2	CVE-2026-18817
cli--cli	GitHub CLI (gh) is GitHub's official command line tool. Prior to version 2.97.0, gh auth status masked only the characters after the last underscore in certain fine-grained personal access tokens and GitHub App tokens. As a result, part of an affected token could appear in terminal or CI output that is captured or shared. Authenticated users are affected if they ran gh auth status (without the --show-token flag) with a token type whose format contains an underscore after the prefix. This includes fine-grained personal access tokens (github_pat_*) and GitHub App installation and user access tokens (ghs_*, ghu_*; for example, ghs_<APPID>_<JWT>), as well as the Actions GITHUB_TOKEN. Classic tokens such as gho_* and ghp_* have an underscore-free body and are not affected. This issue is fixed in version 2.97.0.	2026-08-06	3.3	CVE-2026-64652
DataGear--DataGear	A vulnerability was determined in DataGear up to 5.0.0. The impacted element is the function HtmlTplDashboardWidgetHtmlRenderer of the file HtmlTplDashboardWidgetHtmlRenderer.java of the component Chart Name Handler. This manipulation of the argument Title causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	2.4	CVE-2026-19110
Easy Appointments--Easy Appointments	The Easy Appointments WordPress plugin through 3.12.26 does not correctly validate shortcode input in one of its block-rendering actions, checking only the first tag of the supplied string against an allowlist while rendering the entire string, allowing users with contributor-level access to execute arbitrary registered shortcodes.	2026-08-06	2.7	CVE-2026-14225
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.10, 40.9.0, 41.2.1, and 42.0.0-beta.3, offscreen rendering frame data received from the GPU process was not fully validated by the main process. A compromised GPU process could cause the main process to read out-of-bounds memory while producing paint event images, disclosing memory or crashing the app. This issue is fixed in 39.8.10, 40.9.0, 41.2.1, and 42.0.0-beta.3.	2026-08-05	3.9	CVE-2026-70598
electron--electron	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. Prior to 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3, the native autofill popup could be positioned by a cross-origin iframe outside that iframe's bounds, over the embedding page's UI, enabling clickjacking or spoofing of trusted UI. Apps are only affected if they embed untrusted content in iframes within windows that also display trusted UI. Apps that do not embed untrusted third-party content are not affected. This issue is fixed in versions 39.8.8, 40.9.0, 41.2.1, and 42.0.0-beta.3.	2026-08-05	3.1	CVE-2026-70600
epsilla-cloud--vectordb	A vulnerability has been found in epsilla-cloud vectordb up to 0.3.18/df5a5f5afb85a2376a0f2f316c79dea9b2c6ac7a. This impacts the function SplitTokens/ShuntingYard of the file engine/query/expr/expr.cpp of the component Filter Parser. Such manipulation leads to improper check for unusual conditions. The attack needs to be performed locally. The exploit has been	2026-08-04	3.3	CVE-2026-18852

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
FoundationAgents--MetaGPT	A vulnerability was determined in FoundationAgents MetaGPT up to 0.8.2. This affects the function read of the file metagpt/tools/libs/editor.py. This manipulation causes path traversal. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	3.3	CVE-2026-19059
ggml-org--llama.cpp	A vulnerability was determined in ggml-org llama.cpp e15efe0. Affected by this issue is some unknown functionality of the file common/jinja/parser.cpp of the component Jinja Minja Template Parser. Executing a manipulation with the input {{9 9 }} can lead to reachable assertion. The attack requires local access. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-03	3.3	CVE-2026-18581
HCL Software--HCL iControl	HCL iControl is affected by Missing Access Control vulnerability. The application failed to enforce proper granular access controls, allowing users to access or view administrator-level functionalities without appropriate authorization.	2026-08-03	3.7	CVE-2026-56608
HelloGGX--shadcn-vue-mcp	A weakness has been identified in HelloGGX shadcn-vue-mcp up to e170e277b94235cde627803277fc8c41103a4d38. Affected by this issue is the function fs.promises.readFile of the file src/server/callback-server.ts. This manipulation of the argument filepath causes path traversal. The attack is restricted to local execution. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	3.3	CVE-2026-19324
HKUDS--nanobot	A flaw has been found in HKUDS nanobot up to 0.2.1. The impacted element is the function ExecTool._prepare_command of the file nanobot/agent/tools/shell.py of the component Login-shell Environment Handler. Executing a manipulation can lead to information disclosure. The attack requires local access. The exploit has been published and may be used. Upgrading to version 0.3.0 is sufficient to resolve this issue. This patch is called 4525. The affected component should be upgraded. Multiple issues were reported to the project. They reacted with a high level of professionalism and kindness: "The report concerns shell startup files reintroducing environment variables when command execution defaults to a login shell. The default was changed so exec does not use a login shell unless explicitly requested".	2026-08-07	3.3	CVE-2026-19245
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. From 4.7.0 to 4.12.33, the Proxy Helper proxy() function in hono/proxy does not remove response headers named by the origin's Connection header. Per RFC 9110 Section 7.6.1, an intermediary must remove the header fields listed in a message's Connection header field before forwarding the message, in addition to the well known hop by hop headers, but the proxy() function only removed the well known hop by hop headers, including Connection itself, from origin responses. A client may therefore receive response headers that the origin intended only for its immediate peer, disclosing connection scoped or internal metadata contained in such headers, when an application proxies responses from an origin that declares additional, non standard headers as hop by hop via the Connection response header. This issue is fixed in version 4.12.34.	2026-08-07	3.7	CVE-2026-71849
IBM--Business Automation Workflow containers and traditional	IBM Business Automation Workflow containers and traditional 26.0.0, 25.0.0 through 25.0.0 Interim Fix 005, 24.0.1 through 24.0.1 Interim Fix 007, and 24.0.0 through 24.0.0 Interim Fix 009 IBM Business Automation Workflow fails to properly verify that the hostname matches the server certificate potentially allowing connections to an attacker-controlled server.	2026-08-05	3.8	CVE-2026-12730

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Insta-- InstaKNXServiceApp	A flaw has been found in Insta InstaKNXServiceApp 1.2.3.1469. Affected by this issue is the function CreateWebClientAndDownloadFileList of the component Firmware Update Handler. Executing a manipulation can lead to insufficient verification of data authenticity. It is possible to launch the attack remotely. Attacks of this nature are highly complex. The exploitation is known to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-06	3.7	CVE-2026-19061
Lenovo--XClarity Essentials OneCLI	A temporary file creation vulnerability in the Linux version of Lenovo XClarity Essentials OneCLI 5.5.0 and below could allow a local low-privileged attacker to overwrite or truncate arbitrary local files with program-generated data when OneCLI is executed with elevated privileges.	2026-08-04	3.9	CVE-2026-16791
macrozheng--mall	A flaw has been found in macrozheng mall 0504e86. This vulnerability affects unknown code of the file /sso/getAuthCode of the component mall-portal Module. Executing a manipulation can lead to weak password recovery. The attack may be launched remotely. This attack is characterized by high complexity. It is stated that the exploitability is difficult. The exploit has been published and may be used. The vendor deleted the GitHub issue for this vulnerability without any explanation. Afterwards the vendor was contacted early about this disclosure via email but did not respond in any way.	2026-08-09	3.7	CVE-2026-19361
Meesho--Online Shopping App	A vulnerability was identified in Meesho Online Shopping App up to 20260607 on Android. Affected by this vulnerability is an unknown functionality of the component com.meesho.supply. Such manipulation of the argument user_id/phone number/email address/name leads to cleartext storage of sensitive information. The attack can be executed directly on the physical device. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	2026-08-03	2.1	CVE-2026-18591
mifi--lossless-cut	A vulnerability was determined in mifi lossless-cut up to 3.69.0. Affected by this issue is some unknown functionality of the file src/main/httpServer.ts of the component Built-in HTTP API Service. Executing a manipulation can lead to server-side request forgery. The attack requires access to the local network. This attack is characterized by high complexity. The exploitation is known to be difficult. The exploit has been publicly disclosed and may be utilized. This patch is called 260802348955231442c4bae6c2d9d8ede947af0a. It is best practice to apply a patch to resolve this issue. The project maintainer provides this view: "I'm not sure that this is a critical vulnerability, because it is behind an experimental CLI flag and the NTLM behavior isn't really a LosslessCut bug." The CVSS vector reflects the high level of pre-requisites.	2026-08-09	3.1	CVE-2026-19352
NocteDefensor--LudusMCP	A security vulnerability has been detected in NocteDefensor LudusMCP up to 1.0.24. The impacted element is an unknown function of the file src/tools/ludusEnvironmentGuidesSearch.ts of the component ludus_environment_guides_search. Such manipulation of the argument guide_name leads to path traversal. Local access is required to approach this attack. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-06	3.3	CVE-2026-19046
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.6, the bootstrap challenge endpoint at `/api/tenants/{id}/appointments/bootstrap-challenge` issues a SHA-256 proof-of-work with `difficulty=4` hex zeros, equivalent to 16 bits of work. Modern hardware solves this in under 200 milliseconds, providing essentially no friction against automated abuse of the patient booking flow. Proof-of-work is used in the booking flow as a rate-limiter for unauthenticated clients establishing tunnels and submitting appointments. At 16 bits of difficulty, the construct is decorative rather than effective. An attacker can solve PoW challenges as fast as the server can issue them, defeating the rate-limiting purpose. The handler also calls `challengeThrottleService.checkThrottle(binding, "passkey")`, but the binding	2026-08-06	3.7	CVE-2026-48082

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	includes attacker-controlled values (`tunnelId`, `clientPublicKey`, and optional `emailHash`). For each fresh attempt, the attacker can supply new values, producing a new throttle key and bypassing the per-binding accumulation. Practical abuse friction is therefore the PoW difficulty itself, not a stable per-IP or per-email server-side throttle. Version 1.0.6 fixes the issue.			
open-reception--appointment-booking-software	OpenReception's appointment booking software provides an end-to-end encrypted appointment booking platform. Prior to version 1.0.6, when a TENANT_ADMIN deletes an existing staff user, the underlying `StaffService.deleteStaffMember()` runs an additional invite cleanup that deletes from the central `user_invite` table by email. The `email` clause has no `tenantId` predicate. Any pending invite in any tenant that shares the deleted staff's email is removed. A TENANT_ADMIN of tenant A who deletes a staff record with email `victim[.]example[.]com` also deletes the pending invite for `victim[.]example[.]com` in tenant B, even though they have no relationship to tenant B. The user-side delete is correctly scoped (`eq(user.id, staffId)`, `eq(user.tenantId, tenantId)`), and the pending-invite-only delete path (when `staffId` is itself an invite ID) is also tenant-scoped. The bug is specifically in the invite cleanup that runs as a side effect of deleting an existing staff user. Version 1.0.6 patches the issue.	2026-08-06	2.7	CVE-2026-48074
open-webui--open-webui	Open WebUI is an extensible, feature-rich, and user-friendly self-hosted AI platform. From 0.9.6 until 0.11.0, DELETE /api/v1/chats/{id} cancelled a chat's in-flight tasks before checking whether the caller could delete that chat. Any authenticated user who knew another user's chat id could abort that user's running model response, title generation, or tag generation, even though the delete was refused and no chat data was deleted, modified, or disclosed. This issue is fixed in 0.11.0.	2026-08-04	3.1	CVE-2026-70483
OpenAkita--OpenAkita	A security flaw has been discovered in OpenAkita up to 1.27.12. This vulnerability affects unknown code of the file /api/upload of the component File Upload API. The manipulation of the argument File results in cross site scripting. The attack may be performed from remote. A high complexity level is associated with this attack. It is stated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-03	3.1	CVE-2026-18682
Passter--Passter	The Passster WordPress plugin before 4.3.7 does not restrict low-privilege users holding the edit_posts capability from reading globally password-protected content through the WordPress core REST API when global protection is enabled, allowing any Contributor or higher to read the content of protected pages and posts without knowing the password.	2026-08-06	2.7	CVE-2025-15674
PHPGurukul--Company Visitor Management System	A security vulnerability has been detected in PHPGurukul Company Visitor Management System 1.0. This issue affects some unknown processing of the file /manage-newvisitors.php. The manipulation of the argument fullname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2026-08-07	2.4	CVE-2026-19207
PV-Bhat--gemsuite-mcp	A vulnerability was found in PV-Bhat gemsuite-mcp 1.0.0. Affected by this issue is some unknown functionality of the file src/handlers/unified-gemini.ts of the component gemini_search/gemini_reason/gemini_process/gemini_analyze. The manipulation of the argument file_path/file_paths results in path traversal. The attack must be initiated from a local position. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-09	3.3	CVE-2026-19368
Red Hat--Red Hat Build of Keycloak	A flaw was found in the backchannel logout endpoint of the keycloak-services component, which is part of the Red Hat Build of Keycloak. This component handles authentication and session management for applications. The issue occurs when an OIDC identity provider is configured to skip signature validation. In this specific setup, the system incorrectly accepts logout requests that have no cryptographic signature. An attacker who knows certain technical details about a	2026-08-04	3.7	CVE-2026-18569

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user's session can use this flaw to force that user to be logged out, potentially disrupting their work.			
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in SSSD. The sss_nss_protocol_fill_initgr() function in the NSS responder pre-allocates reply space for all group entries but does not shrink the packet when groups are skipped, causing uninitialized heap bytes to be transmitted to the client. A local attacker can exploit this to disclose cached directory data and heap layout information from the sssd_nss process.	2026-08-04	3.3	CVE-2026-68744
Red Hat--Red Hat Enterprise Linux 10	An injection vulnerability was found in libvirt's virtual network driver. The network XML parser does not strip newline characters from DNS TXT record value attributes and SRV record domain/target attributes. These values are written verbatim into the dnsmasq configuration file generated by the network driver, allowing a user with permission to define virtual networks to inject arbitrary dnsmasq configuration directives such as dhcp-script, leading to arbitrary command execution as root.	2026-08-07	2.3	CVE-2026-61477
rpm-software-management--popt	A flaw was found in poprt, a command-line option parsing library. An off-by-one error in the poprtStuffArgs function, when repeatedly called by a host application or through deep alias nesting, can lead to corruption of internal program data. This corruption could potentially enable a local attacker to execute arbitrary code if the host application then unsafely processes the altered data.	2026-08-04	2.5	CVE-2026-18739
rpm-software-management--popt	An integer underflow was found in the poprt library when formatting help text for option tables that exceed the terminal width. A local user who can cause an application to print help under those conditions may cause that application to crash or fail to display help, resulting in a denial of service of the affected application.	2026-08-05	2.2	CVE-2026-18839
Sharp Corporation--Sharp MFPs	Sharp and Toshiba Tec MFPs (multifunction printers) caches data internally when printing, and leave them uncleared. They may be accessed later by other users.	2026-08-03	2.4	CVE-2026-63545
SourceCodester--Photo Share Website	A flaw has been found in SourceCodester Photo Share Website 1.0. The affected element is an unknown function of the file /social/index.php?page=home. This manipulation of the argument Comment causes cross site scripting. The attack may be initiated remotely. The exploit has been published and may be used.	2026-08-07	3.5	CVE-2026-19209
SourceCodester--Photo Share Website	A vulnerability was identified in SourceCodester Photo Share Website 1.0. This affects an unknown part of the file /social/ajax.php?action=save_upload of the component Comment Input Box. The manipulation of the argument content leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-08-07	3.5	CVE-2026-19230
Systerel--S2OPC	A weakness has been identified in Systerel S2OPC up to 1.7.3. This affects the function LockedStaMac_ProcessMsg_DeleteMonitoredItemsResponse of the file src/ClientServer/frontend/client_wrapper/internal/state_machine.c of the component DeleteMonitoredItemsRequest Handler. This manipulation causes out-of-bounds read. The attack can only be executed locally. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-08-04	3.3	CVE-2026-18790
TBTAK BLGEM Software Technologies Research Institute--pardus-domain-joiner	Unverified ownership vulnerability in TÃfÃ“BÃ„,Ã°TAK BÃ„,Ã°LGEM Software Technologies Research Institute pardus-domain-joiner allows Privilege Abuse. This issue affects pardus-domain-joiner: before 0.5.5.	2026-08-06	3.3	CVE-2026-15599
WonderTrader--WonderTrader	A vulnerability was detected in WonderTrader up to 0.9.9. Impacted is the function TraderDD::queryTrades of the file src/TraderDD/TraderDD.cpp. The manipulation of the argument FID_JYLB results in enforcement of behavioral workflow. The attack can be launched remotely. A high complexity level is associated with this	2026-08-07	3.7	CVE-2026-19208

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attack. The exploitability is considered difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
WSO2--WSO2 Identity Server	The Secret Type Management REST API does not correctly isolate access controls when deleting a secret type. The on-delete cascade logic, when triggered, fails to enforce organizational boundaries, leading to the removal of secrets associated with that type across all organizations. Exploitation of this vulnerability can result in the unintended deletion of secrets across the entire deployment, potentially causing configuration failures, service interruptions, and a denial-of-service condition. This vulnerability requires delete permissions for the Secret Type Management REST API, which are by default only granted to administrators.	2026-08-06	3.8	CVE-2025-14779
WSO2--WSO2 Identity Server	The user impersonation flow in WSO2 Identity Server fails to properly manage refresh tokens associated with impersonated sessions. This allows an attacker who has obtained an access token for an impersonated user to leverage the refresh token grant to obtain new access tokens, extending their ability to act as the legitimate user. An attacker who gains access to an impersonated user's access token can exploit this weakness to renew their authorization. This results in the continued ability to perform actions on behalf of the actual user, compromising log integrity and traceability by masking the true actor.	2026-08-06	2.4	CVE-2025-12627
WSO2--WSO2 Identity Server as Key Manager	When Multi-Attribute Login is enabled, the login interface fails to consistently mask the existence of user accounts. For valid users, the server resolves and displays their canonical username, while for non-existent users, it echoes the original input. This occurs regardless of the validate_username configuration. The discovery of valid usernames can increase the risk of brute force attacks, social engineering attacks, and targeted information leakage. Attackers can leverage this information to craft more effective phishing campaigns or social engineering tactics to compromise user accounts or extract sensitive data.	2026-08-06	3.7	CVE-2025-13736
zephyrproject--zephyr	The kernel queue helper z_queue_node_peek() in kernel/queue.c dereferences a node taken from a queue's data_q list, reading the node's flag byte and, for items enqueued via k_queue_alloc_append/alloc_prepend, the data pointer of an internally allocated alloc_node struct. The implementations of z_impl_k_queue_peek_head() and z_impl_k_queue_peek_tail() performed this read-and-dereference without holding the queue's spinlock, while every other accessor of the same list - including k_queue_get(), which unlinks a node and k_free()s its backing alloc_node - operates under that lock. Because peek was unsynchronized, a concurrent k_queue_get() on the same queue (on an SMP build, or under preemption/ISR concurrency) can free the node between the moment peek obtains the node pointer and the moment it dereferences it. The peek then reads flag bits and a data pointer out of freed, potentially re-allocated heap memory and returns a stale or dangling pointer to its caller. k_fifo and k_lifo are thin wrappers over k_queue, so this affects buffer queues used throughout the net_buf, Bluetooth, USB, and networking subsystems; the peek operations are also system calls reachable from CONFIG_USERSPACE threads. The consequences are a use-after-free read that can leak stale heap contents (one pointer word) and, when the returned dangling pointer is subsequently consumed as a live buffer, a dereference that can crash the system or corrupt memory. Exploitation requires winning a small race window with local access (e.g. a userspace process racing k_queue_peek_* against k_queue_get on a shared queue, or two CPUs), so practical impact is bounded and of low severity. The fix wraps both peek implementations with k_spin_lock/k_spin_unlock on the queue lock, making the read-and-dereference atomic with respect to the concurrent unlink-and-free and bringing peek into line with the rest of the queue's locking discipline.	2026-08-07	3.6	CVE-2026-11742
ZTE--F689	The root password hash of the device can be obtained through unencrypted information in the firmware.	2026-08-07	2.4	CVE-2026-49005

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ZTE--SmartLife	The ZTE Smart Life app contains an SQL injection vulnerability that allows attackers to execute UNION SELECT statements to query sensitive data in the feedback.db database across tables, including user accounts, phone numbers, feedback content, and local debug log paths, thereby enabling the theft of local privacy data.	2026-08-05	3.9	CVE-2026-8029
automad--automad	A vulnerability was determined in automad up to 2.0.0-beta.32. This vulnerability affects the function requestPasswordResetToken of the file automad/src/server/Controllers/API/UserController.php of the component Password Reset Endpoint. This manipulation of the argument name-or-email causes observable response discrepancy. The attack can be initiated remotely. The attack's complexity is rated as high. It is stated that the exploitability is difficult. The exploit has been publicly disclosed and may be utilized. Upgrading to version 2.0.0-beta.33 is able to resolve this issue. Patch name: eac0b05dafdb0ddf8b9139dad8929aaba86568ca. You should upgrade the affected component.	2026-08-17	3.7	CVE-2026-19965
Azuriom--CMS	A weakness has been identified in Azuriom CMS up to 1.2.12. This issue affects the function transferMoney of the file app/Http/Controllers/ProfileController.php of the component Money Transfer Handler. This manipulation causes time-of-check time-of-use. The attack may be initiated remotely. A high degree of complexity is needed for the attack. The exploitability is assessed as difficult. Upgrading to version 1.2.13 is capable of addressing this issue. Patch name: ae5596a9548e010a8a79838806eff60ef9554539. Upgrading the affected component is advised. The vendor was contacted early about this disclosure.	2026-08-17	3.1	CVE-2026-19975
BusyBox--BusyBox	A vulnerability has been found in BusyBox up to 1.30.1. This vulnerability affects unknown code of the file networking/wget.c of the component FEATURE_WGET_TIMEOUT Handler. Such manipulation of the argument -T leads to null pointer dereference. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The name of the patch is 83a40bf7a93c8ac093d33ab45222dd5b9eb57ff. A patch should be applied to remediate this issue.	2026-08-19	3.3	CVE-2026-76014
Combodo--iTop	Combodo iTop is a web based IT service management tool. Prior to 3.2.3, there is sensitive information disclosure in the error messages. This issue has been fixed in version 3.2.3.	2026-08-21	3.5	CVE-2026-33333
Dell--iDRAC9	Dell iDRAC9, versions prior to 7.20.30.50, and Dell iDRAC10, version prior to 1.20.60.50, contain a Remanent Data Readable after Memory Erase vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2026-08-17	3.5	CVE-2026-70412
Dell--ObjectScale	Dell ObjectScale, versions prior to 4.3.0.1, contain(s) a Path Traversal vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2026-08-17	3.3	CVE-2026-56089
drakkan--sftpgp	SFTPGO is an open source, event-driven file transfer solution. From 2.2.0 until 2.7.3, the inline query parameter on browsable-share file downloads and authenticated user-file downloads suppresses Content-Disposition: attachment, allowing an attacker-controlled HTML file stored in a share or home directory to be served as text/html in the SFTPGO web origin. An attacker who can place the file can send a crafted link to a victim, and opening that link executes the stored content in the victim's browser context. Exploitation requires social engineering and suitable share or shared-folder access, while HttpOnly session cookies limit direct cookie theft. This issue is fixed in version 2.7.3.	2026-08-20	3.7	CVE-2026-49245
Esri--Portal for ArcGIS	There is an HTML injection vulnerability in Esri Portal for ArcGIS versions 11.3 and prior that allows a remote attacker with administrative privileges to insert arbitrary HTML into an administrative API. Users working with ArcGIS Enterprise 11.1, and 11.3 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.	2026-08-21	3.8	CVE-2026-69237

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Esri--Portal for ArcGIS	There is an HTML injection vulnerability in Esri Portal for ArcGIS versions 11.5 and prior that allows a remote, highly privileged attacker to insert arbitrary HTML into the Portal for ArcGIS Home application. Users working with ArcGIS Enterprise 11.1, 11.3, and 11.5 are encouraged to patch. All users are advised to upgrade to the latest long-term support release.	2026-08-21	3.5	CVE-2026-69238
Eventin--Eventin	The Eventin WordPress plugin before 4.1.21 does not validate a user-supplied webhook URL stored on events nor verify event ownership, allowing users with contributor-level access and above to trigger blind server-side requests to arbitrary hosts.	2026-08-21	2.7	CVE-2026-13176
filebrowser--filebrowser	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.17, the Link storage struct is serialized directly by sharePostHandler, shareListHandler, and shareGetsHandler through renderJSON, causing POST /api/share/{path} and GET /api/shares to expose password_hash and the bypass token, while an administrator can retrieve these secrets for every user's shares, enabling offline password cracking and direct access to protected shares. This issue is fixed in version 2.63.17.	2026-08-18	2.7	CVE-2026-62684
frangoteam--FUXA	FUXA is a web-based Process Visualization (SCADA/HMI/Dashboard) software. Prior to 1.3.3, DELETE /api/roles removes role definitions through server/runtime/users/usrstorage.js but does not remove the deleted role identifier from each user's info.roles array or the runtime usersMap cache. If a permission configuration still references that identifier, an affected user can retain authorization rights that an administrator intended to revoke, causing residual privilege, inconsistent access-control state, and misleading audit results. This issue is fixed in version 1.3.3.	2026-08-18	2	CVE-2026-67442
freedomofpress--securedrop-client	SecureDrop Client is a desktop app for journalists to securely communicate with sources and handle submissions on the SecureDrop Workstation. Prior to version 1.3.1, a malicious SecureDrop Server could bypass securedrop-proxy's origin limitation by responding with cross-origin redirects. SecureDrop Server itself has multiple layers of built-in hardening, and is a dedicated physical machine exposed on the internet only via Tor hidden services for the Source and Journalist interfaces, and optionally via remote SSH access over another Tor hidden service. A newsroom's SecureDrop Workstation communicates only with its own dedicated SecureDrop Server. Version 1.3.1 fixes the issue.	2026-08-20	3.7	CVE-2026-49996
Huawei--HarmonyOS	UAF vulnerability in the time and time zone module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-08-17	3.3	CVE-2026-49306
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a remote attacker to obtain sensitive information due to a path traversal vulnerability.	2026-08-19	3.7	CVE-2026-16888
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to obtain sensitive information or cause a denial of service due to an integer overflow.	2026-08-19	3.6	CVE-2026-16890
IBM--AIX	IBM AIX 7.2, and 7.3 and IBM PowerVM VIOS 4.1 could allow a local attacker to obtain sensitive information due to an out-of-bounds read.	2026-08-19	3.3	CVE-2026-16891
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to overwrite adjacent memory due to an integer underflow during bounds checking.	2026-08-19	3.5	CVE-2026-18102
jahlives--openssl_encrypt	openssl_encrypt (pip) versions <= 1.4.7 contain an information exposure vulnerability where the 'hsm fido2-test' and 'hsm onlykey-test' diagnostic commands unconditionally print the full derived hardware pepper as hex to stdout/stderr (crypt_cli.py, handle_hsm_command). The printed value can persist in terminal scrollback, session recordings, or CI logs. Impact is limited because the pepper is derived from a random per-invocation test salt and is salt-bound, so the leaked value cannot be used to decrypt real files. A related plugin issue logged raw	2026-08-17	3.3	CVE-2026-74870

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	prf_data outside the secret-redaction path. Fixed in 1.4.8 (and 1.5.0) by removing the hex dumps and routing plugin debug output through the redaction layer.			
jahlikes--openssl_encrypt	openssl_encrypt versions before 1.4.0 contain a logging bug in restore_hidden_modules() that logs module counts after clearing, always showing zero restored modules and corrupting audit trails. Additionally, a race condition exists between module hiding and import hook installation where another thread could re-import blocked modules in multi-threaded environments.	2026-08-17	3.6	CVE-2026-74885
JetBrains--IntelliJ IDEA	In JetBrains IntelliJ IDEA before 2026.2.1 command execution via crafted Markdown preview content was possible in trusted projects	2026-08-17	3.6	CVE-2026-75052
karakeep-app--karakeep	A vulnerability was found in karakeep-app karakeep up to 0.32.0. The affected element is the function authorize of the file apps/web/server/auth.ts of the component Login Endpoint. The manipulation results in improper restriction of excessive authentication attempts. The attack may be performed from remote. This attack is characterized by high complexity. The exploitability is described as difficult. The exploit has been made public and could be used. Upgrading to version 0.33.0 is sufficient to fix this issue. The patch is identified as f7d042971d0d2bcc7119654830cf1eb93eabbf24. It is advisable to upgrade the affected component.	2026-08-18	3.7	CVE-2026-75773
karakeep-app--karakeep	A vulnerability was determined in karakeep-app karakeep up to 0.32.0. The impacted element is an unknown function of the file apps/web/server/auth.ts of the component OAuth Sign-In. This manipulation causes improper authentication. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is regarded as difficult. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2026-08-18	3.7	CVE-2026-75774
Konstanty Bialkowski--libmodplug	libmodplug through 0.8.9.1 contains an out-of-bounds read in pat_smplooped in src/load_pat.cpp. The function validates only the upper bound of its sample index against MAXSMP and then subtracts one before indexing the 191-byte static array pat_loops, so an index of zero reads pat_loops[-1], one byte before the array. The index is the smpno field of a parsed MIDI event, which is initialised to zero and only later overwritten from a program-change parameter, so an event reaching the note test before an instrument is assigned carries zero. A 32-byte MIDI file supplied to the library's public ModPlug_Load entry point drives the path through CSoundFile::Create, CSoundFile::ReadMID, and MID_ReadPatterns to the read. The byte read out of bounds determines whether a note event is treated as looping, so adjacent static storage influences playback state.	2026-08-18	3.3	CVE-2026-75904
Limit Login Attempts Security--Limit Login Attempts Security	The Limit Login Attempts Reloaded WordPress plugin before 3.3.5 does not compare logins against its username denylist case-insensitively and does not account for the account's email address, allowing an account an administrator intended to block from logging in to authenticate anyway.	2026-08-21	3.7	CVE-2026-18356
lin-snow--EchO	A security flaw has been discovered in lin-snow EchO up to 5.4.1. Affected by this issue is the function MD5Encrypt of the file internal/util/crypto/crypto.go. Performing a manipulation results in risky cryptographic algorithm. Remote exploitation of the attack is possible. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 5.4.2 can resolve this issue. The patch is named 9ce19a3b0d0765086a655f45d3a706ec1810404f. It is recommended to upgrade the affected component.	2026-08-20	3.7	CVE-2026-77151
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.6, 10.11.x <= 10.11.21 fail to prevent guest users from receiving Board Admin privileges during board archive import which allows a board member to escalate a guest user to Board Admin via importing a crafted .boardarchive file. Mattermost Advisory ID: MMSA-2026-00672	2026-08-17	3.9	CVE-2026-16044

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.6, 10.11.x <= 10.11.21 fail to enforce run-state validation on write operations for finished playbook runs which allows a run participant to modify status, checklists, retrospective content, ownership, and participants on completed runs via REST and GraphQL API requests. Mattermost Advisory ID: MMSA-2026-00675	2026-08-17	3.5	CVE-2026-16046
Mattermost--Mattermost	Mattermost Plugins versions <=11.8 10.20.11 11.5.7.0 _The Mattermost GitLab plugin fails to verify channel permissions when processing API requests with a caller-supplied_ {{post_id}}_, and fails to validate the_ {{web_url}}_ _parameter against the configured GitLab instance, which allows an authenticated attacker to inject bot-authored messages containing arbitrary URLs into channels they do not have access to via the_ {{createIssue}}_ _and_ {{attachCommentToIssue}}_ _API endpoints._ Mattermost Advisory ID: MMSA-2026-00673	2026-08-17	3.9	CVE-2026-16049
Mattermost--Mattermost	Mattermost Desktop App versions <=6.2 6.2.2.0 fail to redact the pre-auth secret when generating a diagnostics report, which allows a local attacker with access to a user's diagnostics report or log files to obtain the plaintext pre-auth secret configured for a connected server via inspecting the Server Connectivity (Step-3) diagnostics output. Mattermost Advisory ID: MMSA-2026-00716	2026-08-17	3.6	CVE-2026-75587
Mattermost--Mattermost	Mattermost versions 10.11.x <= 10.11.20, 11.7.x <= 11.7.5 Mattermost fails to remove thread membership records when a user is removed from or leaves a team, which allows a previously removed user who is later re-invited to the team to view private channel thread root post content and metadata via the team threads API.. Mattermost Advisory ID: MMSA-2026-00682	2026-08-17	3.5	CVE-2026-9693
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.6, 10.11.x <= 10.11.21 Mattermost failed to restrict OAuth deauthorization and personal access token management endpoints to direct user sessions, which allowed an OAuth app with a delegated user token to revoke the user's authorizations or tokens for other integrations via account-management endpoints.. Mattermost Advisory ID: MMSA-2026-00704	2026-08-17	2.7	CVE-2026-16045
MobSF--Mobile-Security-Framework-MobSF	MobSF is a mobile application security testing tool used. Prior to 4.5.1, get_browsable_activities in mobsf/StaticAnalyzer/views/android/manifest_analysis.py validates only an Android manifest android:host value with valid_host before appending a separately supplied android:port to the URL fetched by _check_url, allowing an authenticated user to upload a crafted APK that makes requests to an attacker-selected nonstandard port at /.well-known/assetlinks.json. With an attacker-controlled hostname and DNS rebinding between validation and the requests.get connection, the request can reach an internal service, although redirects remain disabled and the path is fixed. This issue is fixed in version 4.5.1.	2026-08-18	3	CVE-2026-68927
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the Admin CP Security Questions module does not validate the anti-CSRF token correctly, allowing same-site attackers to enable or disable registration challenge questions with a specially crafted URL. The controller processes GET requests for the disable and enable actions to modify mybb_questions.active without verifying the my_post_key token attached by the user interface. The uniquely identifying implementation details include admin/modules/config/questions.php. This issue is fixed in version 1.8.40.	2026-08-18	3.5	CVE-2026-45126
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the ACP Mass Mail module does not validate certain requests correctly, allowing same-site attackers to create draft entries from archived entries by embedding a specially crafted URL. The Resend route in Admin CP, Users & Groups, Mass Mail, Mass Mailing Archive duplicates archived mailing entries into new drafts with mybb_massemails.status set to 0 on GET requests without request forgery protection. The uniquely identifying implementation details include Users & Groups â' Mass Mail â' Mass Mailing Archive, mybb_massemails.status = 0, and admin/modules/user/mass_mail.php. This issue is fixed in version 1.8.40.	2026-08-18	3.5	CVE-2026-45127

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mybb--mybb	MyBB is free and open source forum software. Prior to 1.8.40, the ACP Users View Manager module does not validate requests correctly, allowing same-site attackers to change a victim administrator's default user list view by embedding a specially crafted URL. The Set as Default control named set_default in Admin CP, Users & Groups, Users, View Manager changes the administrator's default view on GET requests without request forgery protection. The uniquely identifying implementation details include Users & Groups â†’ Users â†’ View Manager, and admin/inc/functions_view_manager.php. This issue is fixed in version 1.8.40.	2026-08-18	3.5	CVE-2026-45128
NixOS--nix	Nix is a package manager for Linux and other Unix systems. Prior to 2.35.0, a malicious derivation executed with the recursive-nix experimental feature can exploit a time-of-check/time-of-use race involving final symlink handling in the LocalStore restore path. The race can cause writeFile to follow a substituted final symlink when opening a path with O_TRUNC instead of enforcing FinalSymlink::DontFollow, allowing the Nix process or nix-daemon to create or truncate an empty file outside the build sandbox with the daemon user's permissions. The primitive does not provide arbitrary-content writes and requires winning the race. This issue is fixed in version 2.35.0.	2026-08-20	2.8	CVE-2026-64846
nlTK--nlTK	NLTK 3.9.4 through 3.10.2 contains a path traversal vulnerability in CrubadanCorpusReader. _load_lang_ngrams joins the corpus root with crubadan_code, the column-0 value read from the corpus table.txt mapping file, and opens the result with the builtin open() rather than the pathsec-validated opener, so os.path.join discards the root when that value is absolute and the read escapes the corpus directory without the containment check nlTK.pathsec applies when ENFORCE is set. An attacker who controls a corpus package can disclose file contents outside the corpus root through lang_freq, limited to paths ending in -3grams.txt whose contents parse as token count lines.	2026-08-22	2.5	CVE-2026-71514
onnx--onnx	Open Neural Network Exchange (ONNX) is an open standard for machine learning interoperability. From 1.3.0 until 1.22.0, onnx.version_converter.convert_version() can perform an out-of-bounds read in Gemm_7_6::adapt_gemm_7_6() in onnx/version_converter/adapters/gemm_7_6.h when a Gemm node has input tensors with fewer than two dimensions because B_shape[1], A_shape[0], or A_shape[1] is accessed without a rank check, potentially causing a process crash during an opset 7 to 6 downgrade. This issue is fixed in version 1.22.0.	2026-08-18	3.3	CVE-2026-63632
OpenStack--Glance	In OpenStack Glance through 32.0.0, the /v2/tasks API accepts type=import tasks that bypass import_filtering_opts, allowing an admin to fetch internal URLs from the Glance service network (aka SSRF), as long as https:// or http:// is used. This API has been available only to admins since Xena, and it has been deprecated for several releases.	2026-08-20	2.2	CVE-2026-77648
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 3.2.20. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Helidon accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	3.7	CVE-2026-60853
Oracle Corporation--Helidon	Vulnerability in the Helidon product of Oracle Fusion Middleware (component: Imperative Web Server). The supported version that is affected is 1.4.20. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Helidon. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Helidon accessible data. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	2026-08-18	3.7	CVE-2026-73923
Oracle Corporation--	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Easily	2026-08-18	3.3	CVE-2026-71072

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Agile PLM MCAD Connector	exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Agile PLM MCAD Connector. CVSS 3.1 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).			
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM MCAD Connector accessible data as well as unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).	2026-08-18	3.7	CVE-2026-71080
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).	2026-08-18	3.3	CVE-2026-71089
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 2.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	2.5	CVE-2026-71082
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 1.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:N).	2026-08-18	1.9	CVE-2026-71081
Oracle Corporation-- Oracle Agile PLM MCAD Connector	Vulnerability in the Oracle Agile PLM MCAD Connector product of Oracle Supply Chain (component: CAX Client). The supported version that is affected is 3.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Agile PLM MCAD Connector executes to compromise Oracle Agile PLM MCAD Connector. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Agile PLM MCAD Connector accessible data. CVSS 3.1 Base Score 1.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N).	2026-08-18	1.8	CVE-2026-71083
Oracle Corporation-- Oracle Hyperion	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation	2026-08-18	3.1	CVE-2026-62461

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Calculation Manager	Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 3.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N).	2026-08-18	3.5	CVE-2026-62529
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with network access via SQL to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data as well as unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	3.8	CVE-2026-62532
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	3.7	CVE-2026-62533
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	3.1	CVE-2026-62604
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	3.1	CVE-2026-62606
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS	2026-08-18	3.7	CVE-2026-70682

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).			
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data as well as unauthorized read access to a subset of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 3.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).	2026-08-18	3.6	CVE-2026-70711
Oracle Corporation-- Oracle Hyperion Calculation Manager	Vulnerability in the Oracle Hyperion Calculation Manager product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion Calculation Manager executes to compromise Oracle Hyperion Calculation Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Calculation Manager accessible data. CVSS 3.1 Base Score 2.6 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	2026-08-18	2.6	CVE-2026-62580
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	3.7	CVE-2026-70848
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 3.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:L).	2026-08-18	3	CVE-2026-70850
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L).	2026-08-18	3.1	CVE-2026-70851
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial	2026-08-18	3.3	CVE-2026-70853

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Management. CVSS 3.1 Base Score 3.3 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:L).			
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data as well as unauthorized read access to a subset of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 3.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	3	CVE-2026-71144
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Management accessible data. CVSS 3.1 Base Score 2.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2026-08-18	2.5	CVE-2026-70919
Oracle Corporation-- Oracle Hyperion Financial Management	Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Financial Management executes to compromise Oracle Hyperion Financial Management. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Financial Management. CVSS 3.1 Base Score 1.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2026-08-18	1.9	CVE-2026-71146
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	3.7	CVE-2026-70785
Oracle Corporation-- Oracle Hyperion Financial Reporting	Vulnerability in the Oracle Hyperion Financial Reporting product of Oracle Hyperion (component: Server). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hyperion Financial Reporting. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Financial Reporting accessible data. CVSS 3.1 Base Score 2.6 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:L/A:N).	2026-08-18	2.6	CVE-2026-70776
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible	2026-08-18	3	CVE-2026-62511

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	data as well as unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 3.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N).			
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Common Security). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 3.3 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:L).	2026-08-18	3.3	CVE-2026-62526
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 3.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).	2026-08-18	3.4	CVE-2026-62569
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 3.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:L).	2026-08-18	3	CVE-2026-62570
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 3.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2026-08-18	3.3	CVE-2026-62577
Oracle Corporation-- Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hyperion Infrastructure Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hyperion Infrastructure Technology. CVSS 3.1 Base Score 3.0 (Integrity and	2026-08-18	3	CVE-2026-62583

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:L).			
Oracle Corporation--Oracle Hyperion Infrastructure Technology	Vulnerability in the Oracle Hyperion Infrastructure Technology product of Oracle Hyperion (component: Installation and Configuration). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hyperion Infrastructure Technology executes to compromise Oracle Hyperion Infrastructure Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Infrastructure Technology accessible data. CVSS 3.1 Base Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	3.3	CVE-2026-70962
Oracle Corporation--Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u501, 11.0.32, 17.0.20, 21.0.12, 25.0.4, 26.0.2; Oracle GraalVM for JDK: 17.0.20 and 21.0.12; Oracle GraalVM Enterprise Edition: 21.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-08-18	3.7	CVE-2026-60589
Oracle Corporation--Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.14. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).	2026-08-18	3.4	CVE-2026-71140
Orange View Limited--DualSafe Password Manager & Digital Vault Extension	A flaw has been found in Orange View Limited DualSafe Password Manager & Digital Vault Extension up to 1.4.35 on Chrome. Affected is an unknown function of the component postMessage-based Bridge. Executing a manipulation can lead to information disclosure. The attack can be launched remotely. A high complexity level is associated with this attack. The exploitability is told to be difficult. The exploit has been published and may be used. The vendor was contacted early about this disclosure.	2026-08-17	3.1	CVE-2026-19992
ridafkih--keeper.sh	keeper.sh's calendar module version prior to 2.18.14 contains a server-side request forgery (SSRF) guard bypass vulnerability that allows authenticated attackers to reach private network addresses by exploiting a DNS rebinding attack against the two-phase URL validation and connection flow. The SSRF guard validates a hostname's resolved IP addresses but discards them before the actual HTTP connection is opened, allowing an attacker who controls authoritative DNS to return a public address during validation and a private address during the subsequent independent socket-level DNS resolution, causing the guard to pass while the outbound connection reaches internal infrastructure such as cloud instance metadata endpoints.	2026-08-19	3.5	CVE-2026-75583
romkatv--powerlevel10k	powerlevel10k fails to neutralize control characters in the package.json version field when rendering the package prompt segment. Attackers can inject raw escape	2026-08-17	3.3	CVE-2026-75483

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bytes in the version string to emit arbitrary terminal control sequences on each prompt render when the shell enters affected directories.			
SEIKO EPSON CORPORATION--Multiple SEIKO EPSON printers and scanners	Multiple SEIKO EPSON printers and scanners contain revoked root certificates. A man-in-the-middle attack may allow an attacker to obtain communication data transmitted by the product. As for the details of the affected products and versions, refer to the vendor's information.	2026-08-20	3.7	CVE-2026-73542
Splunk--FireAMP	In FireAMP versions below 2.1.15, a user who holds a role that can edit, create, or run playbooks in Splunk SOAR could run the add listitem action in a Safe Mode playbook while that action is listed as read-only, which could allow for unauthorized changes to file lists. The vulnerability is possible because the FireAMP connector action manifest classifies the add listitem action as read-only even though the action updates file lists. For more information see Manage settings for a playbook in Splunk SOAR (https://help.splunk.com/en/splunk-soar/soar-cloud/build-playbooks/manage-playbooks-and-playbook-settings/manage-settings-for-a-playbook-in-splunk-soar-cloud) in the Splunk documentation.	2026-08-19	2.7	CVE-2026-76371
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.9, and 9.4.14, a user who holds a Splunk role that contains the high-privilege list_search_head_clustering capability could send a read request to Search Head Cluster member control endpoints and change cluster state, which could allow for a denial of service. The vulnerability is possible because the Search Head Cluster member control endpoints do not require a state-changing Hypertext Transfer Protocol (HTTP) request type before they apply read-only authorization.	2026-08-19	3.8	CVE-2026-76348
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user with the "Administrator" role could use the /rest/support/connectivity/.../check_connectivity endpoint to make Splunk SOAR initiate outbound network connections to arbitrary destinations and determine whether internal hosts and ports are reachable. The Server-Side Request Forgery (SSRF) is possible because the connectivity check REST API does not sufficiently validate the destination before Splunk SOAR connects to it. For more information see Manage roles and permissions in Splunk SOAR (On-premises) (https://help.splunk.com/en/splunk-soar/soar-on-premises/administer-soar-on-premises/8.5.0/manage-your-splunk-soar-on-premises-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-on-premises) in the Splunk documentation.	2026-08-19	2.7	CVE-2026-76361
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user who holds a role that contains the playbooks:view permission could view metadata about a playbook repository that they are not authorized to view. The vulnerability is possible because Playbook History does not check repository permissions before returning playbook revision metadata. For more information see Manage roles and permissions in Splunk SOAR (Cloud) (https://help.splunk.com/en/splunk-soar/soar-cloud/administer-soar-cloud/manage-your-splunk-soar-cloud-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-cloud) and Manage settings for a playbook in Splunk SOAR (Cloud) (https://help.splunk.com/en/splunk-soar/soar-cloud/build-playbooks/manage-playbooks-and-playbook-settings/manage-settings-for-a-playbook-in-splunk-soar-cloud) in the Splunk documentation.	2026-08-19	2.7	CVE-2026-76368
Splunk--Splunk SOAR	In Splunk SOAR versions below 8.6.0, a user who holds the OnPrem Broker role could write files outside the intended Automation Broker log directory. The vulnerability is possible because Automation Broker log uploads accept crafted filename input before writing log files. For more information see Manage roles and permissions in Splunk SOAR (Cloud) (https://help.splunk.com/en/splunk-soar/soar-cloud/administer-soar-cloud/manage-your-splunk-soar-cloud-users-and-accounts/manage-roles-and-permissions-in-splunk-soar-cloud) and About Splunk SOAR Automation Broker (https://help.splunk.com/en/splunk-soar/splunk-	2026-08-19	2.7	CVE-2026-76369

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	automation-broker/about-splunk-soar-automation-broker/about-splunk-soar-automation-broker) in the Splunk documentation.			
Systerel--S2OPC	A vulnerability has been found in Systerel S2OPC up to 1.7.3. Impacted is the function SOPC_NodeMgtHelperInternal_AddVariableNodeAttributes of the file src/ClientServer/address_space/internal/sopc_node_mgt_helper_internal.c of the component AddNodes Service. The manipulation of the argument UserAccessLevel leads to out-of-bounds read. It is possible to initiate the attack remotely. A high degree of complexity is needed for the attack. The exploitability is considered difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is aafbd37d381b618312ebdf5ddf57027f62c14fdd. It is suggested to install a patch to address this issue.	2026-08-22	3.7	CVE-2026-78049
Tanium--Findings	Tanium addressed a compression bomb vulnerability in Findings.	2026-08-19	3.1	CVE-2026-11617
Tanium--Threat Response	Tanium addressed a compression bomb vulnerability in Threat Response.	2026-08-19	3.1	CVE-2026-75476
torproject--Tor	tor before 0.4.9.9 was prone to an infinite loop when decompressing a truncated zlib/gzip stream with done=1. A truncated stream never reaches Z_STREAM_END, causing zlib to return Z_BUF_ERROR with no input remaining, which buf_add_compress() mistook for a full output buffer and retried forever. Fixed by returning TOR_COMPRESS_ERROR in that case so the caller can abort cleanly. This is TROVE-2026-021.	2026-08-20	3.7	CVE-2026-77640
Webkul--Bagisto	A vulnerability was determined in Webkul Bagisto up to 2.4.4. This affects an unknown part of the file /customer/account/rma/send-message of the component RMA Message Handler. This manipulation of the argument Message causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The vendor confirms: "The reported issues were already identified through our internal security assessment process prior to this notification and are being handled through our established internal security and development lifecycle. Some of these items have already been addressed, while the remaining items are planned for resolution in upcoming product releases."	2026-08-17	3.5	CVE-2026-19995
Wireshark Foundation--Wireshark	ERF file parser crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	3.1	CVE-2026-76884
Wireshark Foundation--Wireshark	Tektronix K12xx file parser crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	3.1	CVE-2026-76885
Wireshark Foundation--Wireshark	Crash in the Wireshark dissection engine in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	3.1	CVE-2026-76887
Wireshark Foundation--Wireshark	RDP protocol dissector crash in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	3.1	CVE-2026-76888
Wireshark Foundation--Wireshark	Crash in sharkd in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	3.1	CVE-2026-76890
Wireshark Foundation--Wireshark	Crash in sharkd in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	3.1	CVE-2026-76891

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Wireshark Foundation-- Wireshark	BUSMASTER file parser abnormal exit in 4.6.0 to 4.6.7 and 4.4.0 to 4.4.18 allows denial of service	2026-08-19	3.1	CVE-2026-76926
Yamaha Corporation-- VOCALOID6	Missing authentication for critical function vulnerability exists in VOCALOID6. Any process running under the same local user account as a running VOCALOID6 Editor instance may escalate privileges via a local named pipe.	2026-08-21	3.3	CVE-2026-76137